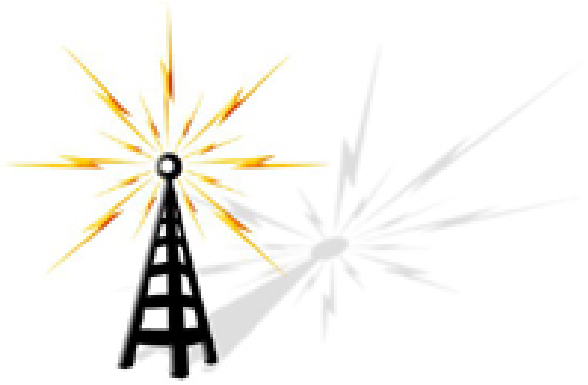
Star OS V3



Valemount Networks Corporation

Lonnie Nunweiler, President

Copyright 2006, Valemount Networks Corporation and David A. Bandel, all rights reserved.

FCC Regulatory Compliance

All Lucaya Wireless Advanced Routers have been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Users are cautioned that any changes or modifications to the Lucaya Wireless Advanced Routers can void the user's authority to operate the equipment.

Harmful interference generated by use of this equipment must be mitigated by the user/installer at their own expense.

All operators should utilize good safety practices when installing and operating this equipment.

Table of Contents

Getting Started....7
Section 1....7
Loading your system....7
Installing via RAW image....7
Upgrading from V2....7
Booting up StarOS....7
Section 2....8
Initial Configuration....8
Entering your license key....8
Changing your password....10
Changing Network information....11
Setting up your wireless card....12
WEP Setup....15
Activating Changes....15
On bridges and routers....17
The Main Window....19
The Menu Bar....19
Generic Information....20
System Information....20
Serial Number....20
Service Summary....20
Wireless Devices....21
The Information Bar....21
File and System Menus....22
Section 1....22
File Menu....22
Save changes....22
Activate changes....23
Reboot....23
Exit....23
Section 2....24
System menu....24
Services....25
Configure background color....28
Change password....28
Update / Enter License Key....28
Upgrade firmware....28

SSH client....28
Telnet client....28
System Console....29
The Interfaces Menu....31
Configuring Interfaces....31
Ether and Wireless Cards....31
Device submenus....32
IP assignments....32
Wireless Configuration....34
Config current card....34
Enable....34
ESSID....35
BSS Channel....35
Custom Checkbox and Scan List....35
Transmit Rate (mbps)....36
Link distance (0..35 miles)....36
Country code....36
Tx Power Override (0..30 dbm)....36
Cloaking....37
Antenna Select....37
Hide SSID....37
InterBSS Relay....38
Outdoor Only....38
Short Preamble....38
Super A/G....38
AP Power Saving Mode....38
Network Type....38
Operating Mode....38
Available Channels Window....38
WEP Security submenu....39
Access Control List Editor....39
Client List....40
Site Survey....42
Ethernet Configurations....43
Ethernet Link Settings....43
Interface Features....44
DHCP auto-auth configuration....44
Beacon real-time traffic monitor....47
DHCP Client Information....48
802.1q Virtual Lan (VLAN) Setup....48

Virtual Distribution System (VDS) Setup....50
Creating an Ethernet Bridge....50
Routing Menu....52
Configuring routing....52
Static and default routes....52
Dynamic Routing....53
Policy and Advanced Routing....56
Advanced Menu....57
Configuration notes....57
Static ARP....58
802.1d Bridging Options....59
DNS Server List....60
Connection Tracking Setup....61
Connection Table Size....62
NTP and Zone configuration....63
Remote Syslog....64
System Log....65
The Scripts Dropdown Submenu....66
Class Based Queueing script....67
Advanced Firewall and Port Forwarding script....68
NAT and Static NAT....69
System Reports....70
The CBQ Traffic Report....71
View System Information....72
Active PPP user list....73
Network Utilities....74
Ping Utility....75
Ping response....76
tcpdump Utility box....77
tcpdump response box....78
Throughput Test Box....79
Throughput Test Response Box....80
Configuration, Upgrades, Tips and Tricks....81
starutil....81
Saving and restoring configurations....82
Upgrading....82
Tips and Tricks....83
Wireless Practices....84
Your radio....84
Your tower....84

Cables....85
Ethernet/POE cables....85
Antenna cables....86
Antennas....86
Calculations....87
Appendix 1
StarOS Country Codes....89
Codes sorted alphabetically by digraph....89
Codes sorted alphabetically by country....92
Appendix 2
Network Primer....95
Introduction....95
Background....95
IP....95
NETMASK....96
VLSM Notation....97
Subnetting....97
Adjacent and Contiguous....98
Finding the network....99
Routing....99

Chapter 1

Getting Started

This chapter will deal with your first exposure to StarOS v3. Section 1 will show you how to load StarOS onto your WRAP or WAR board or upgrade your board from V2 to V3. Section 2 will then take you through a few first essential steps so you can start using your StarOS router. All attempts have been made to make getting started as easy as possible. The same can be said about subsequent chapters, but only you can judge how successful we've been.

Section 1

If your system has been preloaded by an OEM or StarOS VAR or reseller, feel free to skip ahead to Section 2.

Loading your system

The easiest way to load StarOS onto a system is to visit the StarOS downloads page at http://www.staros.com/downloads.php and download the latest version of the software for the system you want.

You can load StarOS v3 onto any media, but only compact flash will be discussed here. If you've purchased WAR boards from Gateworks, you will need a special JTAG cable available from Gateworks to load the OS. Please see the instructions provided with the downloaded WAR image for details.

Installing via RAW image

If you choose to write a raw image to disk, you'll need to boot into the operating system of your choice and use a program suitable for writing the raw image to the disk. Install the disk you want StarOS written to and boot up. Using a program such as DiskImg.exe in Windows, or dd in Linux, BSD, or other UNIX clones/systems write the raw disk image to the appropriate disk: dd if=vncOs-1.1.0-1338.X86-WRAP.cf of=/dev/hde bs=512.

Upgrading from V2

You can use starutil to upgrade from V2 to V3, but you first need to ensure you flash up to strrw-2.11.1-4784.co.bin. From there you need to install the new license prior to installing and booting into V3. Please refer to the instuctions for using the starutil utility on page 80.

Booting up StarOS

After writing your disk, you'll just need to make sure it's installed as the first hard disk in your system and you will boot up directly into StarOS. After booting, you'll have a few housekeeping chores to do which are covered in the next section.

Section 2

Initial Configuration

Once the system starts, you can log in from a console or via SSH on your network. By default, StarOS will start up with the default IP 192.168.1.1 on the first ethernet port and a default gateway of 192.168.1.254.

You need to login via SSH (ssh or dropbear client in UNIX or putty.exe in Windows) and use the username admin with password 1234. You'll be greeted with a trial screen (unless an activation key was entered for you). <Alt>+l or <ESC> will close the screen and present you with the main StarOS screen (see fig 0).

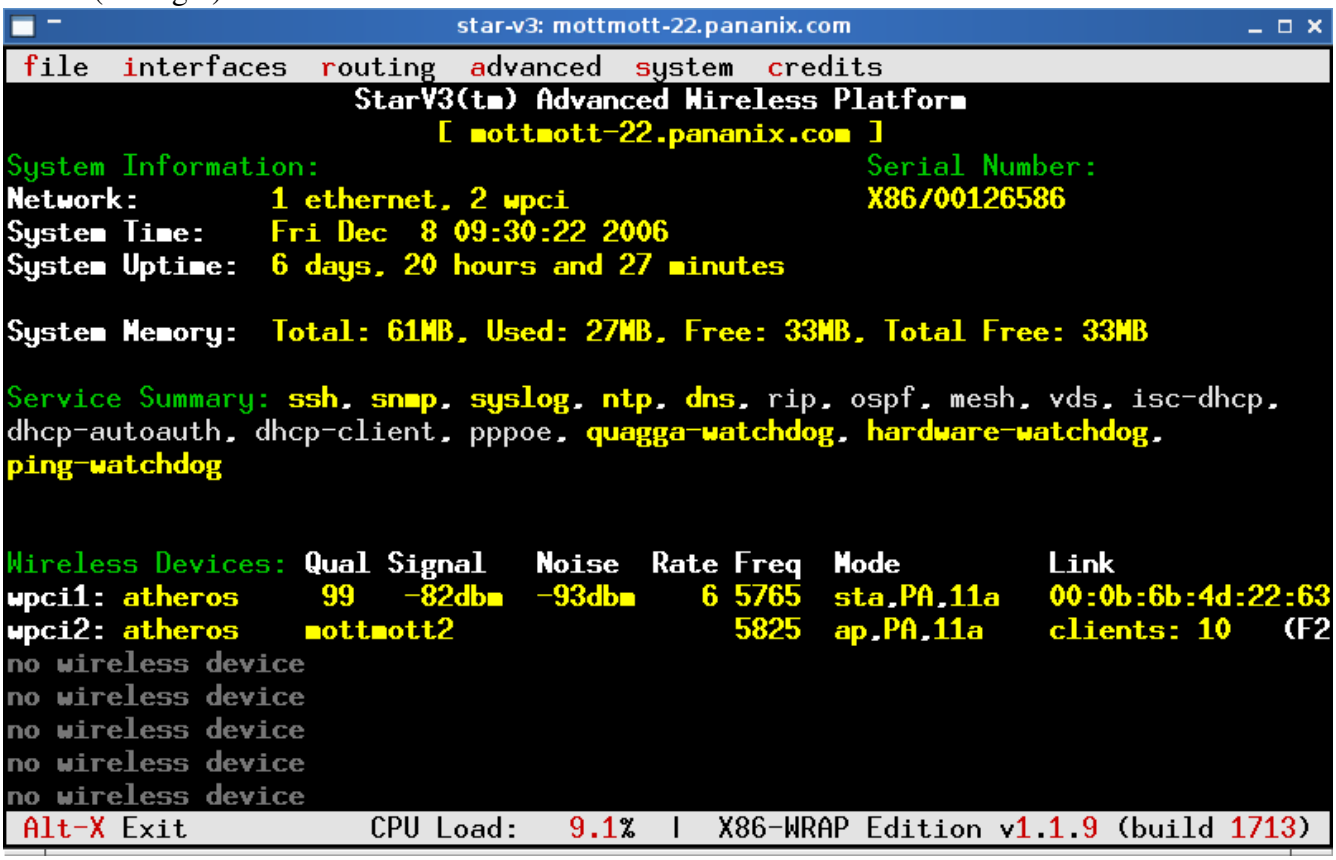

star-v3: mottmott-22.pananix.com
file interfaces routing advanced system credits
StarV3(tm) Advanced Wireless Platform
[mottmott-22.pananix.com]
System Information:
Serial Number:
Network: 1 ethernet, 2 wpci
X86/00126586
System Time: Fri Dec 8 09:30:22 2006
System Uptime: 6 days, 20 hours and 27 minutes
System Memory: Total: 61MB, Used: 27MB, Free: 33MB, Total Free: 33MB
Service Summary: ssh, snmp, syslog, ntp, dns, rip, ospf, mesh, vds, isc-dhcp, dhcp-autoauth, dhcp-client, pppoe, quagga-watchdog, hardware-watchdog, ping-watchdog
Wireless Devices: Qual Signal Noise Rate Freq Mode Link
wpci1: atheros 99 -82db -93db 6 5765 sta,PA,11a 00:0b:6b:4d:22:63
wpci2: atheros mottmott2 5825 ap,PA,11a clients: 10 (F2
no wireless device
no wireless device
no wireless device
no wireless device
no wireless device
Alt-X Exit CPU Load: 9.1% | X86-WRAP Edition v1.1.9 (build 1713)

fig0: Initial StarOS screen

Entering your license key

If you do not have a system key entered, using your mouse, select System (<Alt>+s) then item 4 enter / update unlock key from the drop down box. Selecting Get Request Key will provide you with a number that you must use to request a license key (see figs 1 and 2). The license key is tied to your MAC address.

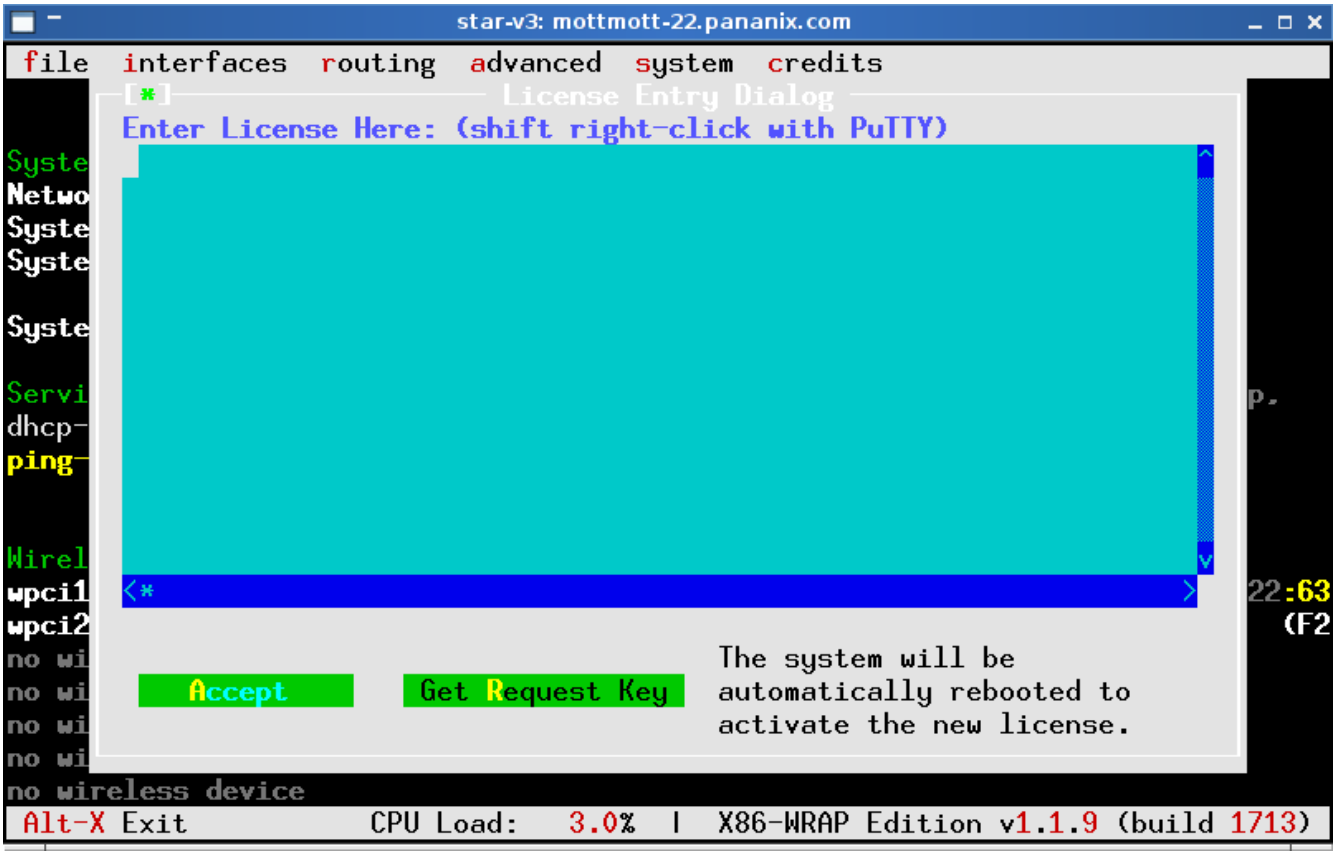

star-v3: mottmott-22.pananix.com
file interfaces routing advanced system credits
License Entry Dialog
Enter License Here: (shift right-click with PuTTY)
Accept
Get Request Key
The system will be automatically rebooted to activate the new license.
no wireless device
Alt-X Exit
CPU Load: 3.0%
X86-WRAP Edition v1.1.9 (build 1713)

fig 1: License Entry Dialog

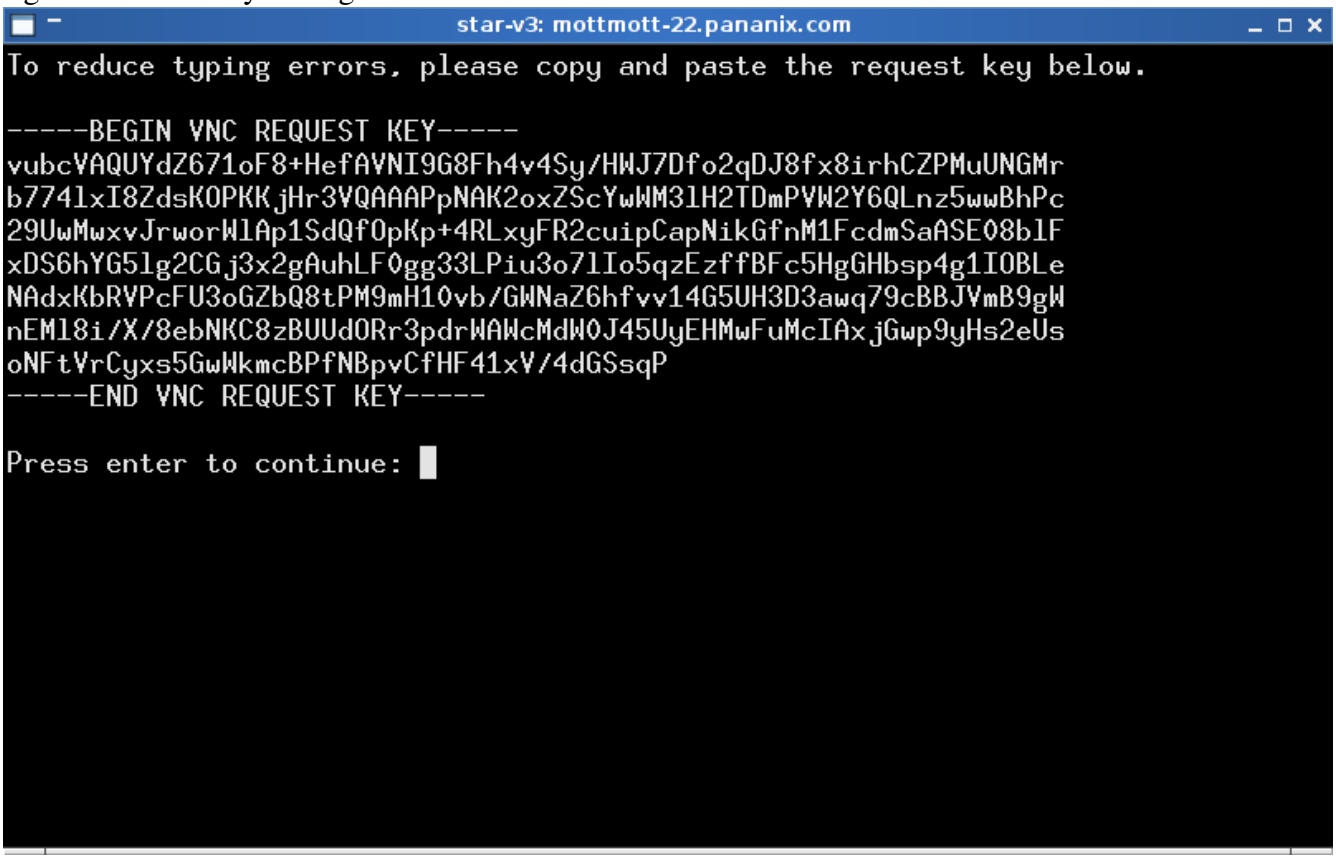


fig 2: Sample VNC Request Key screen

In Windows, you should be able to use a shift+left mouse button and drag to select, and shift+right mouse button to paste. In UNIX using X, you'll need to experiment, but shift+left mouse button and drag selects, and shift+middle mouse button for paste has worked for me. This may be window manager dependent, your mileage may vary.

The unlock key will be a GPG-type key. Just paste into the box and select Accept. Include the lines -----BEGIN and -----END

Record your unlock key in case your disk is damaged (your key will be e-mailed to you if you have a valid address on file).

Changing your password

All access to the StarOS system is via the user admin. Changing the default admin password is a very good idea, and doing so as soon as possible is your best insurance against unauthorized entry. Select System -> Change password (see fig 3). You'll be presented with a box asking you for the old password. Enter 1234. Then enter your new password. It will not be shown on the screen, but you'll be asked to confirm it to ensure you didn't mistype it. If you lose your password, you'll have to reload the system or revert the system to its factory default via the serial port, so remember it (Note: not all WAR boards have a serial connector). Chapter 11 will show you how to save your configuration in case you have to reload, but you will still need to know the admin user's password.

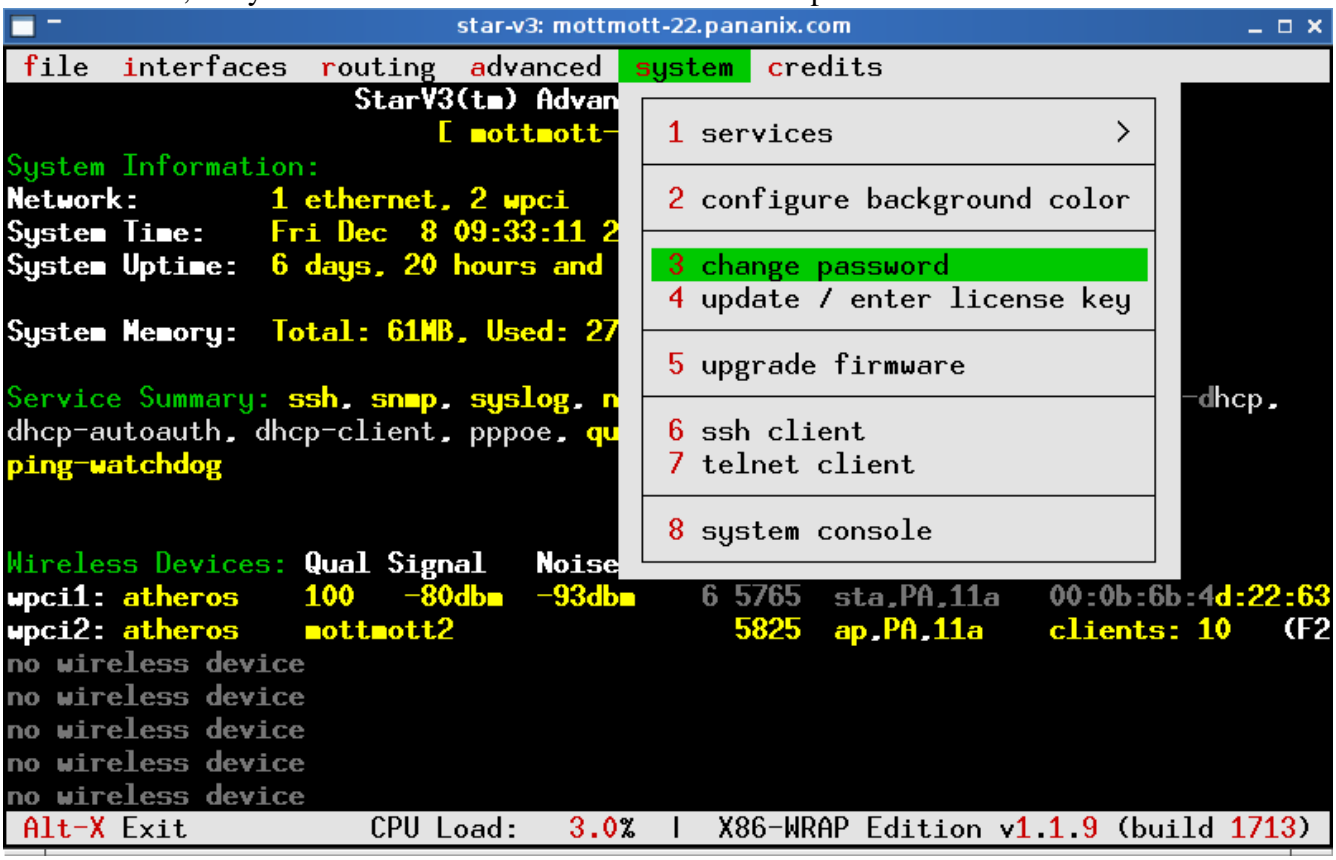

star-v3: mottmott-22.pananix.com
file interfaces routing advanced system credits
StarV3(tm) Advan
[mottmott-
System Information:
Network: 1 ethernet, 2 wpci
System Time: Fri Dec 8 09:33:11 2
System Uptime: 6 days, 20 hours and
System Memory: Total: 61MB, Used: 27
Service Summary: ssh, snmp, syslog, n
dhcp-autoauth, dhcp-client, pppoe, qu
ping-watchdog
-dhcp,
1 services >
2 configure background color
3 change password
4 update / enter license key
5 upgrade firmware
6 ssh client
7 telnet client
8 system console
Wireless Devices: Qual Signal Noise
wpci1: atheros 100 -80dbm -93dbm 6 5765 sta,PA,11a 00:0b:6b:4d:22:63
wpci2: atheros mottmott2 5825 ap,PA,11a clients: 10 (F2
no wireless device
no wireless device
no wireless device
no wireless device
no wireless device
Alt-X Exit CPU Load: 3.0% | X86-WRAP Edition v1.1.9 (build 1713)

fig 3: System menu

Changing Network information

Select interfaces -> ether1 -> ip assignments to change the IP address. The box will allow you to create, remove, edit, or disable/enable an IP address. You can tab between fields if not using a mouse, or use the <Alt>+hotkey combination to select the appropriate field. (see fig 4)

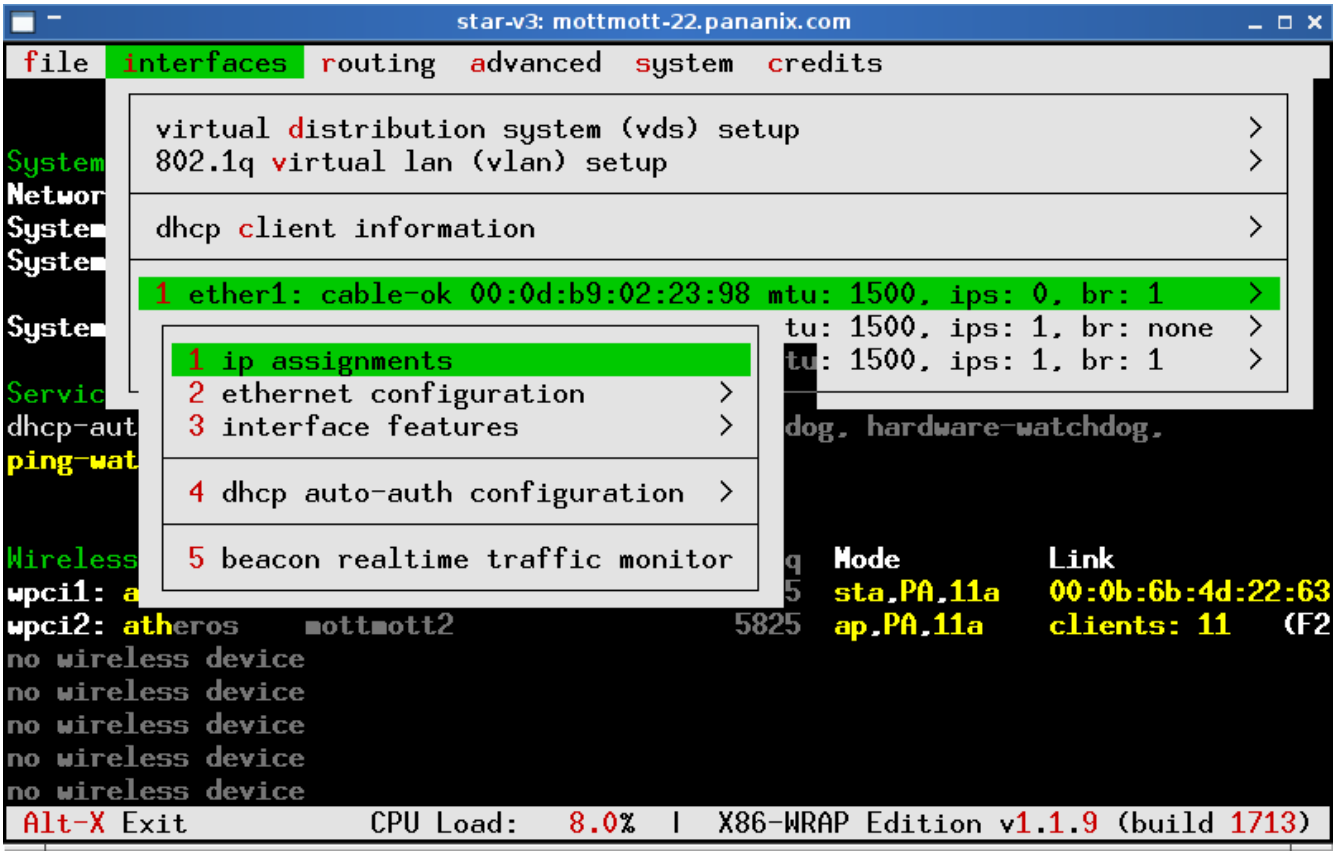


fig 4: Interfaces menu

While here, look at the bottom of the box labeled “Ethernet Bridge Number (1-9, 0=disabled)”. By default, the StarOS system, unlike most wireless systems, is a router, not a bridge. If you want this system to act like most most APs, CPEs, or wireless bridges on the market, you'll want to change this box from 0 to 1. (see fig 5) For an explanation of routers versus bridges, see “A note about bridging” later in this chapter. When you're finished, hit the <ESC> key to get out.

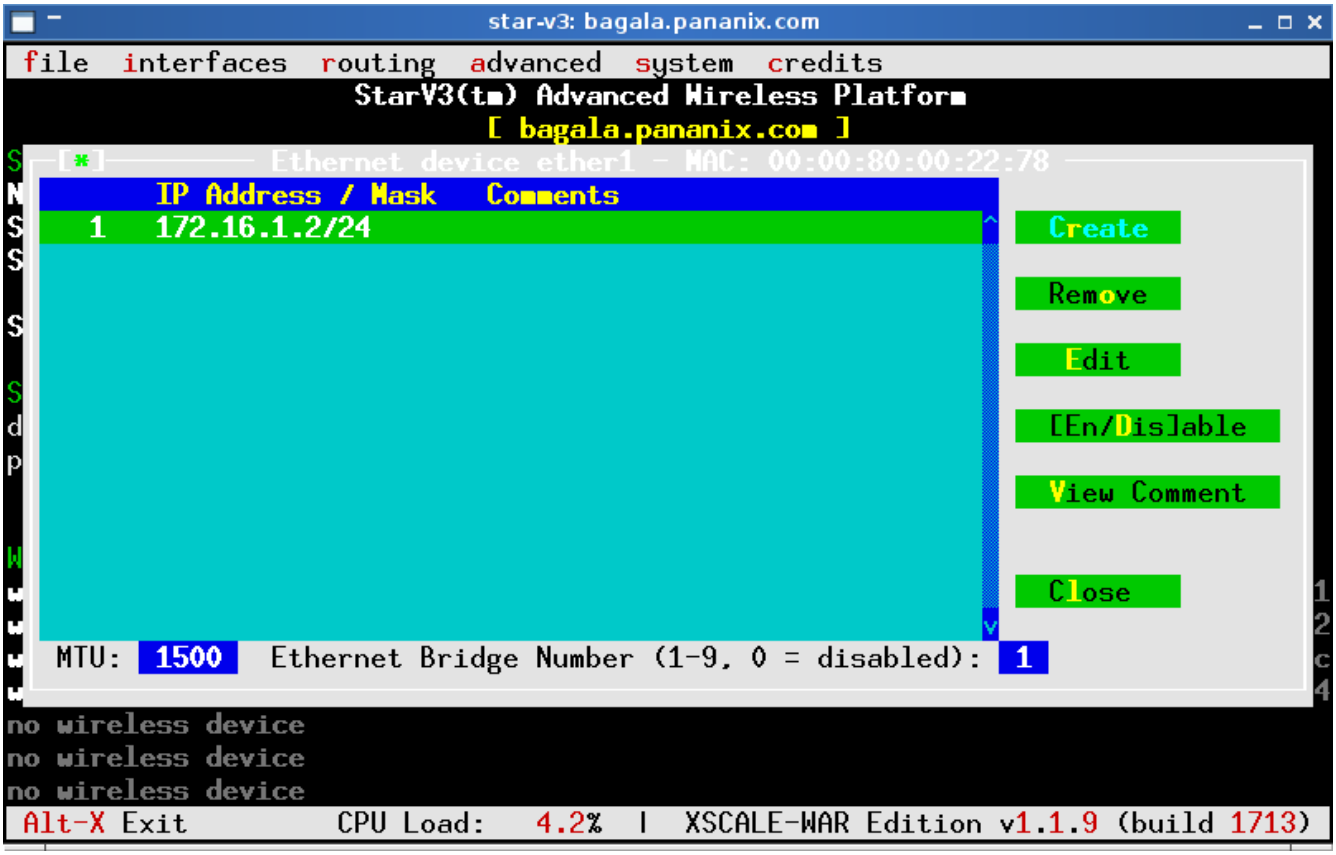


fig 5: device configuration screen

If you've made this interface part of a bridge, you'll want to include other interfaces as part of the bridge, so select interfaces -> wpci1 (substituting your desired bridge interface here) -> ip assignments, and put a 1 in the Ethernet Bridge box.

Now go to the routing drop-down and select static and default routes. Edit the gateway to correspond to the gateway of the IP you assigned to the Ethernet interface. For more details, see page 38.

Setting up your wireless card

Now set up your wireless card by selecting the interfaces drop-down, then your wireless interface (wpci#)->wireless configuration -> configure current card. (see fig 6 and fig 7) First ensure the card is enabled. You may change the ESSID if you desire. If this is an access point, you'll need to configure the BSS Channel.

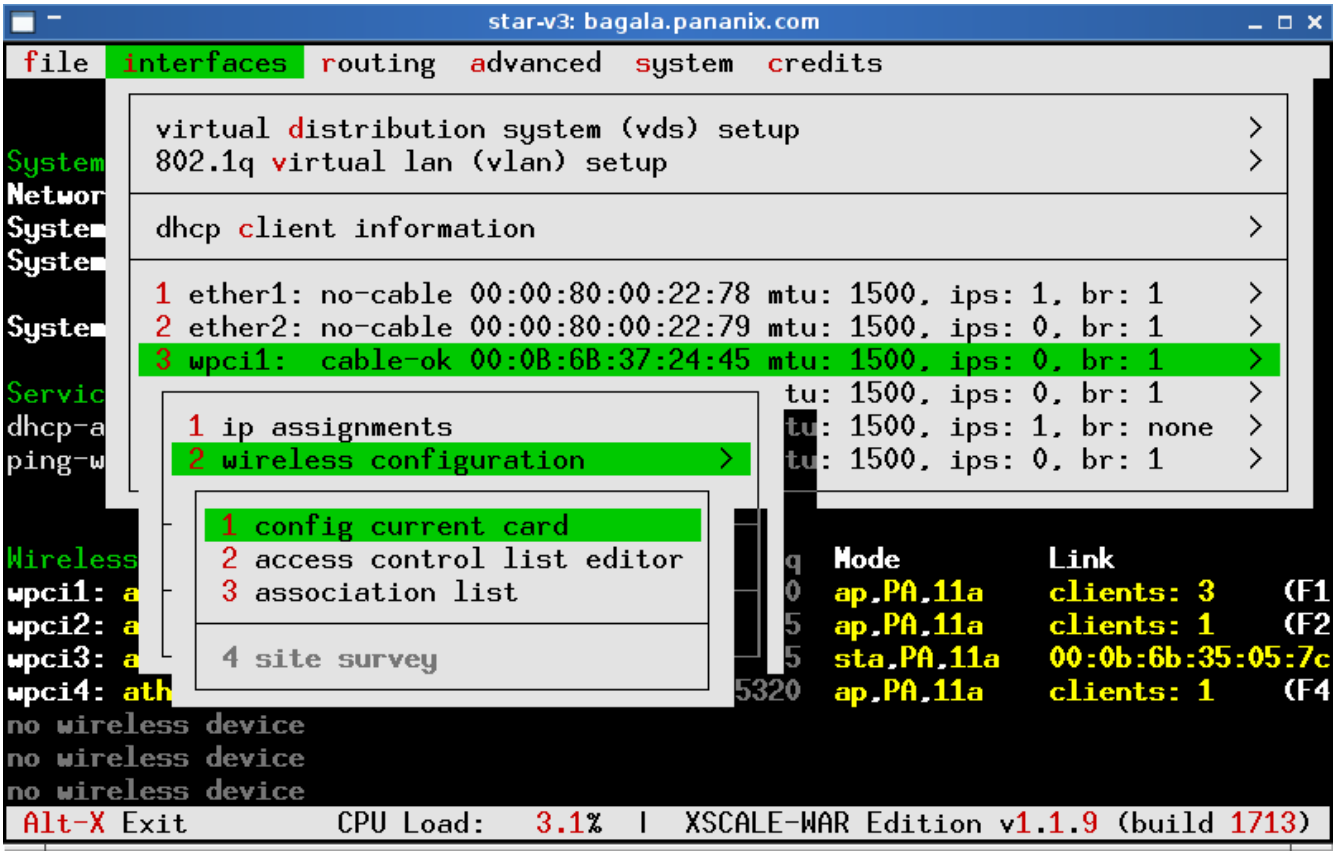

star-v3: bagala.pananix.com
file interfaces routing advanced system credits
virtual distribution system (vds) setup
802.1q virtual lan (vlan) setup
dhcp client information
1 ether1: no-cable 00:00:80:00:22:78 mtu: 1500, ips: 1, br: 1
2 ether2: no-cable 00:00:80:00:22:79 mtu: 1500, ips: 0, br: 1
3 wpci1: cable-ok 00:0B:6B:37:24:45 mtu: 1500, ips: 0, br: 1
1 ip assignments
2 wireless configuration
1 config current card
2 access control list editor
3 association list
4 site survey
Mode
Link
wpci1: ap,PA,11a clients: 3 (F1
wpci2: ap,PA,11a clients: 1 (F2
wpci3: sta,PA,11a 00:0b:6b:35:05:7c
wpci4: ath ap,PA,11a clients: 1 (F4
no wireless device
no wireless device
no wireless device
Alt-X Exit CPU Load: 3.1% | XSCALE-WAR Edition v1.1.9 (build 1713)

fig 6: wireless dropdown

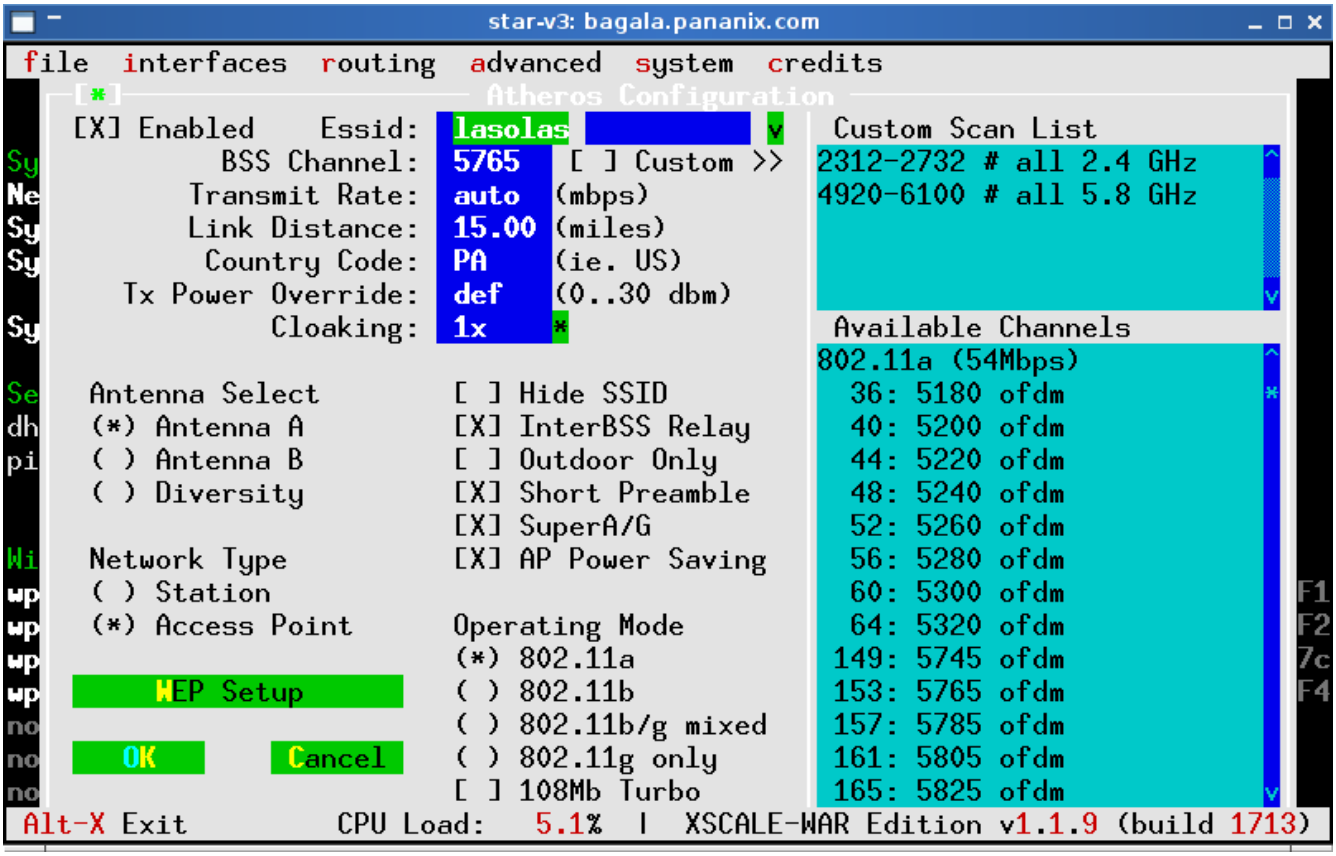


fig 7: wireless configuration

The BSS channel can be either a channel number (as shown in the Available Channels box to the right) or the frequency in megahertz. You must select a valid channel number or frequency. Selecting an invalid channel number or frequency will result in the system using the lowest frequency in that range.

The Custom checkbox will force the system to use only those frequencies shown in the Custom Scan List. You can remark out the entries and put select frequency lists (one list or frequency per line). This will limit client scans to only listed frequencies and will also affect the frequencies displayed in the Available Channels box.

For now, leave the transmit rate at "auto", although later you may want to change your access point to lock in a rate so weak stations don't slow the network down. Transmit rate will depend on the frequency and mode selected, but will be one of: 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54, 72, 96, or 108.

The link distance is very important. This number determines how long the system will wait after sending frames to its neighbors before assuming they are lost. If this number isn't greater than the distance in miles to the farthest station, stations beyond this range will handshake, but not pass data. This means that if a remote station is set with a number too low, you won't be able to communicate with it to change the distance – you'll have to go to the remote site to fix it, so make sure you adjust the local radio to its shortest distance first.

The country code should be entered per the list in Appendix A. This code will determine what frequencies and channels are shown in the Available Channels window.

The transmit power override window will allow you to increase or decrease the power leaving the radio card for the antenna. This may be set as "def" (default), 0 (same as default) or 1 to 30. Not all frequency ranges allow the full 1W output. This is a function of the card, not StarOS. Atheros cards run 18db by default.

Ensure you select the correct antenna. For the most part, that should be Antenna A (the connector in the upper corner of the card). If you have two pigtails connected to one card, you can use the diversity antenna setting with a spatial diversity antenna.

The Hide SSID turns off AP broadcasts of your ESSID. While this will help hide you from war drivers, it should not be considered adequate by itself to secure your network.

The InterBSS Relay option, when checked, allows clients to talk client-to-client through the AP.

The Outdoor Only box will reduce the number of channels in the Available Channels box by removing lower powered (by regulation) channels.

The Short Preamble box should only be checked if you can control all clients connected to you. Older cards may only understand the long preamble. Hot Spots will definitely not want to check this box.

The Super A/G will use compression techniques and other methods to increase speed. Like the short preamble box, super A/G will discriminate against older, slower clients.

AP Power Saving mode can lower power consumption when the AP is not actively passing traffic. If you have a solar-powered site, you will want to check this.

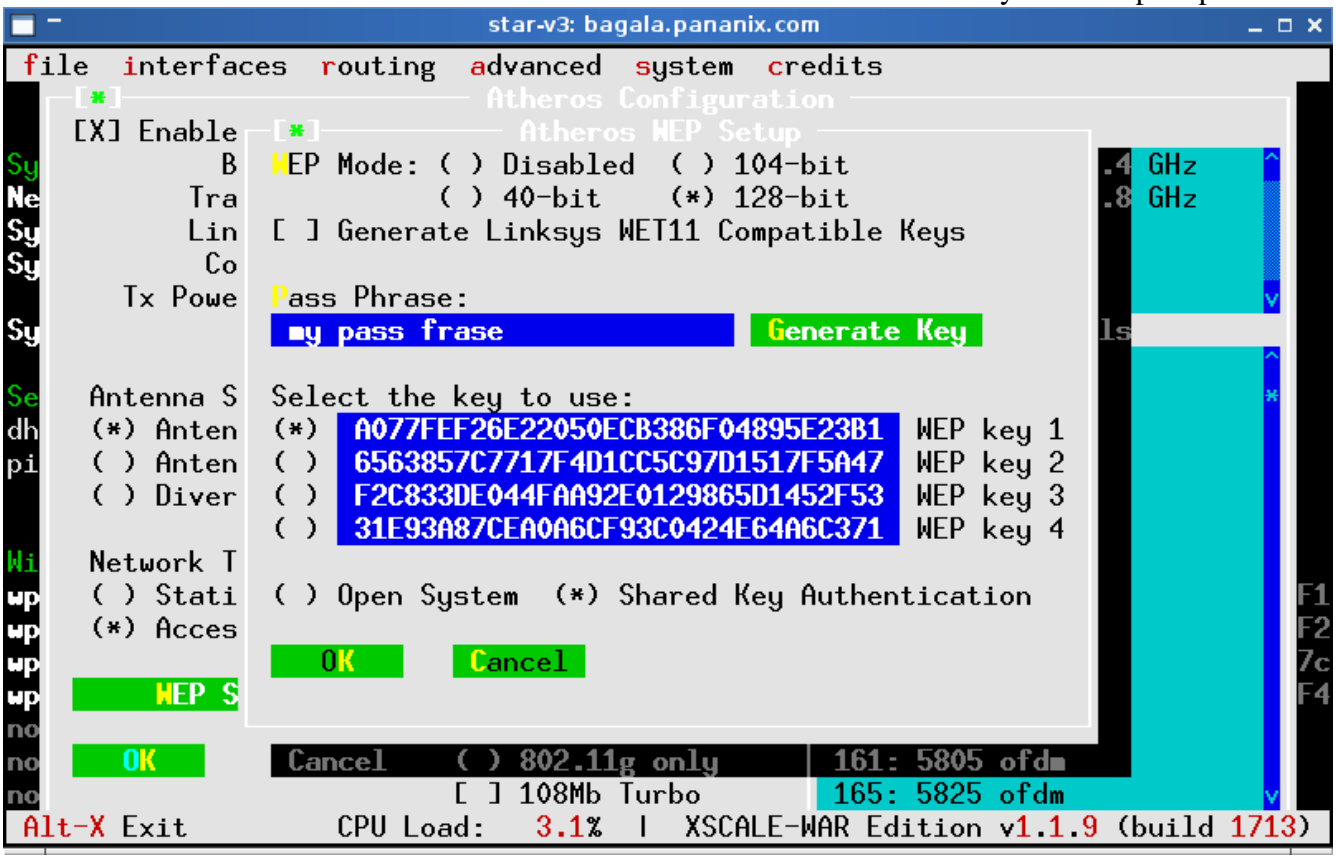
The Network Type determines whether the system will act as a client or Access Point. Point-to-point only is not supported. However, if you need a wireless bridge, see page 39, Creating an Ethernet Bridge.

Operating mode determines if you are operating as 8011.b (2.4GHz DSSS), 802.11g (2.4GHz OFDM), or 802.11a (5.x GHz OFDM), a mixed or homogeneous b/g network, and whether these modes use turbo mode or not (802.11g and 802.11a only).

The Available Channel window is informational and will only change after a country is selected, then the changes are activated (see Activating Changes below). The frequencies in this box will also be affected by entries in the Custom Scan List.

WEP Setup

Selecting WEP Setup will present the box shown in fig 8. The Wireless Encryption Protocol will make breaking into your system harder (but not impossible). By default it is disabled. Select the key size you want (if you have Microsoft Windows clients, choose either 40 or 104 bit encryption). If you use the same pass phrase and select Generate Key, your keys will all be identical. So you can have good keys without the need to memorize them or write them down. Just use the same key size and pass phrase.

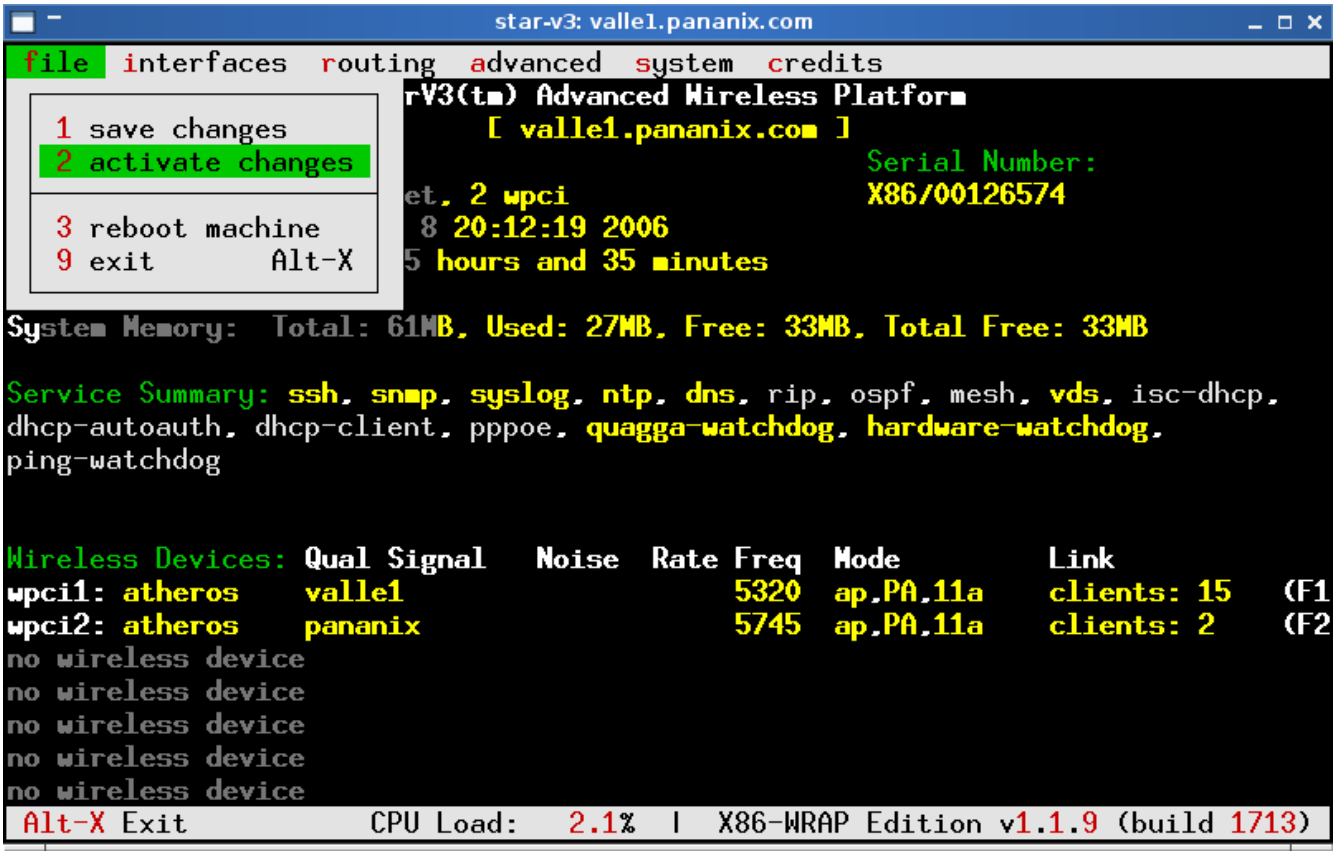

star-v3: bagala.pananix.com
file interfaces routing advanced system credits
Atheros Configuration
Atheros WEP Setup
[X] Enable
WEP Mode: ( ) Disabled ( ) 104-bit
( ) 40-bit (*) 128-bit
[ ] Generate Linksys WET11 Compatible Keys
Pass Phrase:
my pass frase
Generate Key
Select the key to use:
(*) A077FEF26E22050ECB386F04895E23B1 WEP key 1
( ) 6563857C7717F4D1CC5C97D1517F5A47 WEP key 2
( ) F2C833DE044FAA92E0129865D1452F53 WEP key 3
( ) 31E93A87CEA0A6CF93C0424E64A6C371 WEP key 4
( ) Open System (*) Shared Key Authentication
OK
Cancel
( ) 802.11g only
[ ] 108Mb Turbo
161: 5805 ofdm
165: 5825 ofdm
Alt-X Exit
CPU Load: 3.1%
XSCALE-WAR Edition v1.1.9 (build 1713)
fig 8: WEP setup

Also select either Open System or Shared Key Authentication.

Activating Changes

After you've done all the above, you're ready to begin testing your system. The changes made above will only get you started. You've probably noticed nothing has actually changed yet. Changing the IP address didn't disconnect you. So you'll need to activate the changes you made above.

Select the File pull-down menu (see fig 9). In it you'll see: save changes, activate changes, reboot machine, and exit. You may save your changes at any time. You may activate changes without saving them to ensure that they work properly before saving them permanently, or you can reboot the machine.


star-v3: valle1.pananix.com
file interfaces routing advanced system credits
1 save changes
2 activate changes
3 reboot machine
9 exit Alt-X
rV3(tm) Advanced Wireless Platform
[valle1.pananix.com]
Serial Number:
X86/00126574
et, 2 wpci
8 20:12:19 2006
5 hours and 35 minutes
System Memory: Total: 61MB, Used: 27MB, Free: 33MB, Total Free: 33MB
Service Summary: ssh, snmp, syslog, ntp, dns, rip, ospf, mesh, vds, isc-dhcp, dhcp-autoauth, dhcp-client, pppoe, quagga-watchdog, hardware-watchdog, ping-watchdog
Wireless Devices: Qual Signal Noise Rate Freq Mode Link
wpci1: atheros valle1 5320 ap,PA,11a clients: 15 (F1
wpci2: atheros pananix 5745 ap,PA,11a clients: 2 (F2
no wireless device
no wireless device
no wireless device
no wireless device
no wireless device
Alt-X Exit CPU Load: 2.1% | X86-WRAP Edition v1.1.9 (build 1713)
fig 9: file dropdown

Both activate changes and reboot machine will prompt you to save any changes. If you say No, a reboot will reset the system to its state just after the last time you saved your configuration. This, combined with the system -> services -> ping watchdog, can save you a long trip if a change you made prevents access to a remote system.

On bridges and routers

Most wireless systems are bridges by design. They learn about systems and IPs on each side and pass packets between two network segments. Bridges look like switches. They do not appear in a traceroute. In fact, they can be thought of as an electronic extension of the Ethernet cable that connects them to the rest of the network. Bridges do not require IP addresses themselves, and it's easier to understand what they are if we think about them as if they didn't have IP addresses. But it certainly makes administration of the systems easier when they do have IP addresses.

Routers, on the other hand, have multiple IP addresses, always have IP addresses on two or more networks, and have routing tables that tell them which interface to send packets on to send them on their way. These routing tables can be static (hand made) or dynamic (built using software such as quagga that monitors the network and talks to neighboring routers via one of RIP, BGP, OSPF, or other routing protocols). Routers do show up in traceroutes.

Routers route packets between networks, and bridges span network segments into one network segment. Therein lies the problem with bridges. Wireless bridges in particular offer an easy way to create loops Except for the simplest of networks using wireless bridges, spanning tree protocol (STP) should always

be implemented to ensure packets don't run around in circles accidentally (STP is enabled by default in StarOS). Bridges are also not as scalable as routers. If you anticipate extensive growth, you might be better served starting off using routing.

Another problem with wireless bridges is that while APs are true bridges, clients are psuedo-bridges and use proxy arp to simulate a bridge. A large network behind a client can cause all manner of odd problem, generally systems that can't find other systems until the remote system sends a packet in. A work-around is available that will overcome this and will be discussed in depth in the Interfaces section as VDS.

In subsequent chapters, I will also discuss software in terms of its utility on either a routed or bridged network. For example, dhcp relays are required in routers, but not in bridges. So an understanding of network topology becomes necessary as a wireless network expands.

Chapter 2

The Main Window

This chapter will look at information presented on the main screen. (see fig 1) This information will differ slightly depending on your equipment and its function. So we'll look at what information is presented and its importance to your wireless network.

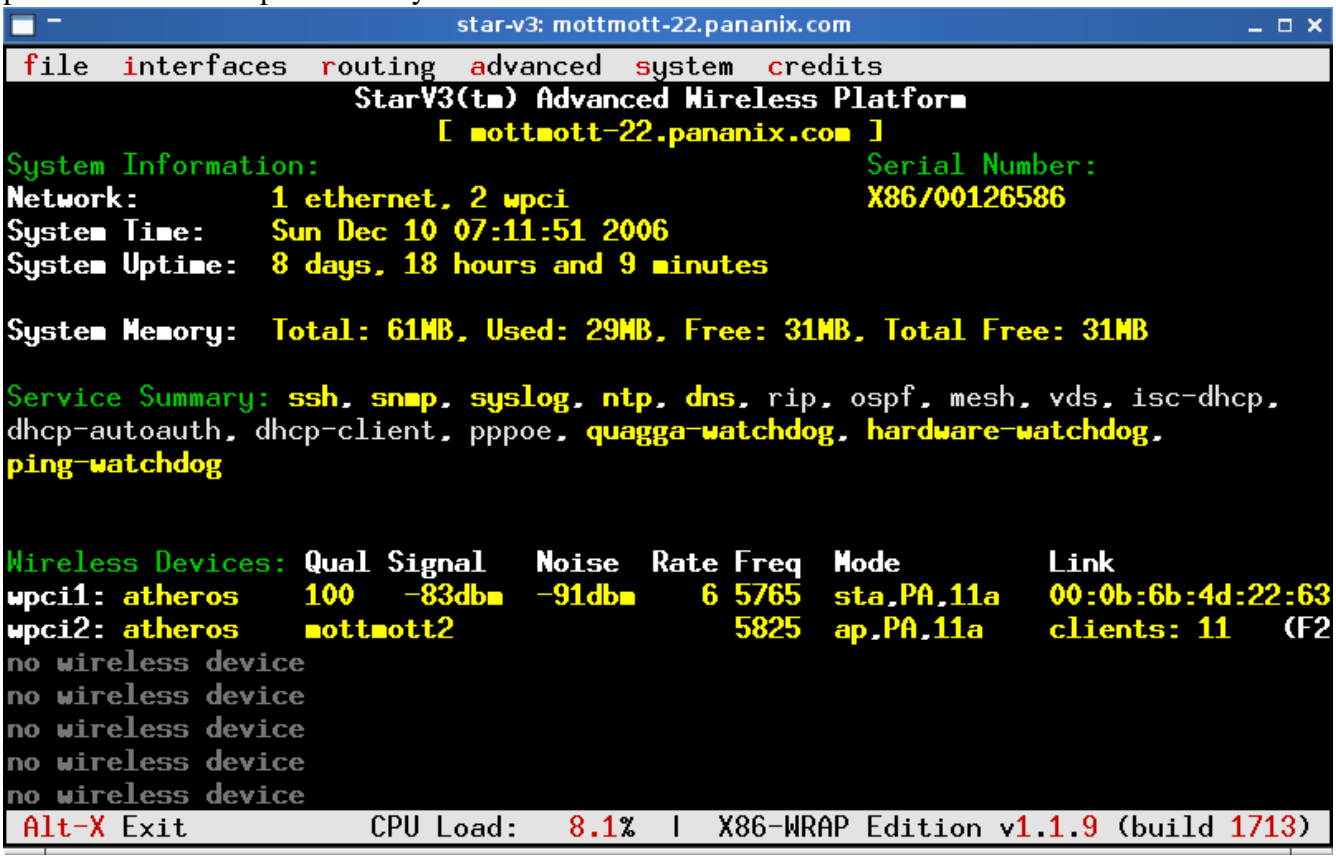

star-v3: mottmott-22.pananix.com
file interfaces routing advanced system credits
StarV3(tm) Advanced Wireless Platform
[mottmott-22.pananix.com]
System Information:
Serial Number:
Network: 1 ethernet, 2 wpci
X86/00126586
System Time: Sun Dec 10 07:11:51 2006
System Uptime: 8 days, 18 hours and 9 minutes
System Memory: Total: 61MB, Used: 29MB, Free: 31MB, Total Free: 31MB
Service Summary: ssh, snmp, syslog, ntp, dns, rip, ospf, mesh, vds, isc-dhcp, dhcp-autoauth, dhcp-client, pppoe, quagga-watchdog, hardware-watchdog, ping-watchdog
Wireless Devices: Qual Signal Noise Rate Freq Mode Link
wpci1: atheros 100 -83dbm -91dbm 6 5765 sta,PA,11a 00:0b:6b:4d:22:63
wpci2: atheros mottmott2 5825 ap,PA,11a clients: 11 (F2
no wireless device
no wireless device
no wireless device
no wireless device
no wireless device
Alt-X Exit CPU Load: 8.1% | X86-WRAP Edition v1.1.9 (build 1713)

fig 1: main window

The Menu Bar

The menu bar allows access to all of the StarOS configuration functions. Anything you can do or configure, you'll find in the menu bar.

The menu bar can be activated using either your mouse or keyboard shortcut keys. The red letters indicate the shortcut keys. So to open the file dropdown menu, you can either select file with your mouse (assuming you're using an xterm or in Windows, putty) or you can use <Alt>+f. Once activated, you may continue to use the shortcut keys or mouse, or you can navigate using the arrow keys on your keyboard.

Generic Information

Below the menu bar, you'll see information regarding StarOS. Normally this will be StarV3(tm) Advanced Wireless Platform.

Below the brand should appear the system name inside square brackets. This is the fully qualified domain name (hostname.domain.tld) of your system and can be changed by selecting Advanced -> dns server list. In the hostname: box put just the hostname of the system. In the domain box put the domain name with the top level domain. Below that fill in the IP addresses of your DNS servers. Unless you've activated the local caching DNS server (system menu -> services -> dns server), you should change 127.0.0.1 to the address of another DNS server.

System Information

The System Information area consists of 4 items. These items are self-explanatory but included so that you can orient yourself quickly and easily.

The Network information comes from the kernel and the identifying names of the various network devices in the system.

The System Time should be updated via the Advanced menu -> ntp and timezone setup area. In order to ensure your radios all have the same time, you should slave them off a local NTP server. A wise choice would be your radius server or DNS server. Otherwise, any server accessible to all systems is fine. Under Linux or BSD, ntp, openntp, or chrony are good choices as ntp servers.

System uptime gives you a good idea of how long since the system reboot. If you find the system rebooting under load, you may have a power problem i.e., insufficient power for your system. Radios demand more power under load. Try using a higher wattage power supply (watts = volts * amps). So either obtain a power supply that will provide more amps at the same voltage, or if you're using POE (power over ethernet), reduce the length of cable from the power injector to the radio.

System memory shows how much RAM memory you have and are using. Remember your total memory might show less than you expect. For example, a 64MB RAM system may show only 61MB total. This is what has been allocated to the system.

Serial Number

The serial number just shows what your system serial number is and that it has a license. StarOS version 3 can be run in licensed mode or unlicensed mode. The unlicensed mode provides basic features. The basic features are configuration of the ethernet devices (but not radios), the VLAN and VDS functions. Note the serial number and save it. Should something happen to your system, you can reload the license key that goes with that system.

Service Summary

The service summary area shows you at a glance which services are running. Running services are shown in yellow and unused services are shown in gray. Some services cannot (and should not) be

turned off. Most of these services have corresponding items in one of the menus, but some don't (at least not directly).

Wireless Devices

The wireless devices header section lists Qual(ity), Signal, Noise, Rate, Freq(uency) Mode, and Link Information. In client mode, all these fields will contain associated information. In AP mode, less information is shown, link specific details can be found in the Interfaces -> wpci# -> wireless configuration-> client list.

The first column lists the wireless device (wpci# or wlan#). This is followed by the specific radio device.

Quality refers to percentage of packets not retransmitted. This provides a quick indication of how well or poorly the link is running. A high number of retransmits (low percentage number) indicates a very poor link. On APs, this column will contain the ESSID name.

The Signal column shows signal strength (client only). This number will be negative.

The Noise column (also a negative number) shows background noise level (limited by the driver and speed – client only). The difference between signal and noise is the signal to noise ratio (SNR). The SNR which is easily calculated by looking at the signal and noise numbers gives an indication of how strong a signal your system hears.

The Rate column (client only) indicates the wireless speed. This number will show you the wireless (not network) connection speed. The specific speeds that will be displayed here depend on operating mode (802.11a, 802.11b, 802.11g, and turbo mode for those that support it). These speeds may change during the course of communications if speed is set to auto in the wireless configuration.

The Freq column shows the frequency the system is transmitting/receiving on.

The Mode will consist of three comma separated fields. The first field indicates mode of operation, one of ap or sta (for Access Point or Station). The second field shows the configured country code. The third field shows the frequency operating mode, one of 11a, Ta, 11b, 11bg, Tg, 11g.

The Link information will provide either the number of associations or the system MAC address.

The Information Bar

The information bar on the bottom of the screen provides at a glance a number of things. It provides a quick way to logoff. It also provides the CPU load. Finally, the information bar shows you the firmware you're running.

Chapter 3

File and System Menus

This chapter will address the two smallest dropdown menus, the File menu dropdown and the System menu dropdown. These two dropdowns are among the smallest, but most important of the dropdowns.

Section 1

File Menu

The file menu dropdown will be one of your most used dropdowns as you configure and test your system. Nearly all functions will require activation to make the system start using them (see fig 1).

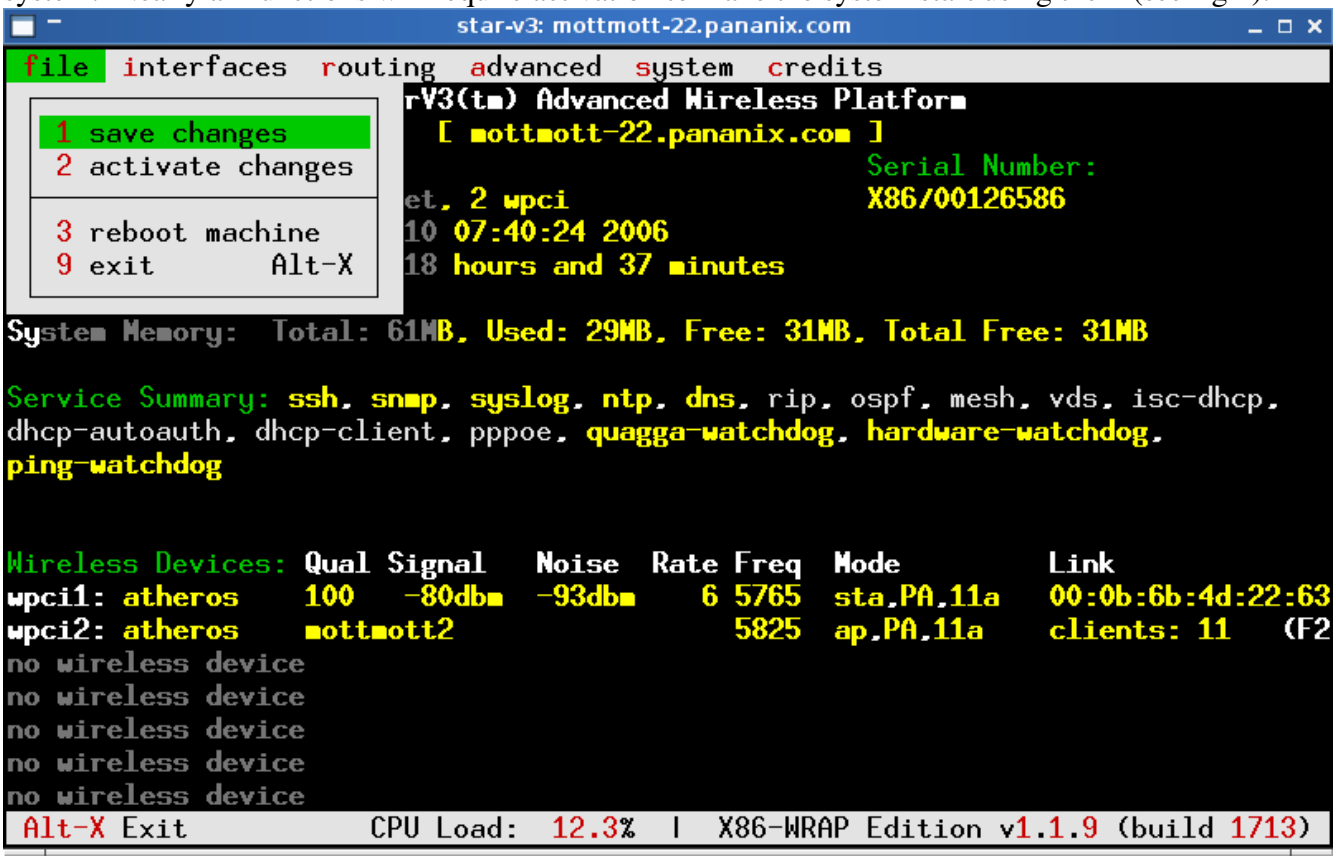

star-v3: mottmott-22.pananix.com
file interfaces routing advanced system credits
1 save changes
2 activate changes
3 reboot machine
9 exit Alt-X
rV3(tm) Advanced Wireless Platform
[mottmott-22.pananix.com]
Serial Number:
et, 2 wpci
X86/00126586
10 07:40:24 2006
18 hours and 37 minutes
System Memory: Total: 61MB, Used: 29MB, Free: 31MB, Total Free: 31MB
Service Summary: ssh, snmp, syslog, ntp, dns, rip, ospf, mesh, vds, isc-dhcp, dhcp-autoauth, dhcp-client, pppoe, quagga-watchdog, hardware-watchdog, ping-watchdog
Wireless Devices: Qual Signal Noise Rate Freq Mode Link
wpci1: atheros 100 -80dbm -93dbm 6 5765 sta,PA,11a 00:0b:6b:4d:22:63
wpci2: atheros mottmott2 5825 ap,PA,11a clients: 11 (F2
no wireless device
no wireless device
no wireless device
no wireless device
no wireless device
Alt-X Exit CPU Load: 12.3% | X86-WRAP Edition v1.1.9 (build 1713)

fig 1: file dropdown

Save changes

The save changes option in the file menu does exactly as its name implies. It will save the changes you've made to the system. These changes will not take effect immediately only be saved. You must either reboot or activate your saved changes for them to take effect. There are a few menu items that don't require activation but become active immediately. These will be noted in future chapters. So the save menu will allow you to save those changes for them to carry over between reboots.

Activate changes

After making a change that is not immediate in nature, you must activate it for it to take effect. When selected, you will be presented a dialog box asking if you want to save the changes, not save the changes, or cancel. Not saving the changes permits you to test a feature that may disconnect you when activated. This option, combined with the system -> services-> ping watchdog, will allow you to recover access to a remote system should the new configuration not work as anticipated. If all works well, a quick save changes will save the configuration through a reboot.

Reboot

This option does exactly what it says, but also presents you a dialog box asking if you want to save your configuration or not. A reboot is required to make your system begin using a new timezone if you changed the offset under the advanced -> ntp and timezone setup menu.

Exit

Will exit your login session. Logout is immediate.

Section 2

System menu

While not often used, the system menu is, nonetheless, important as it changes essential parameters (see fig 2).

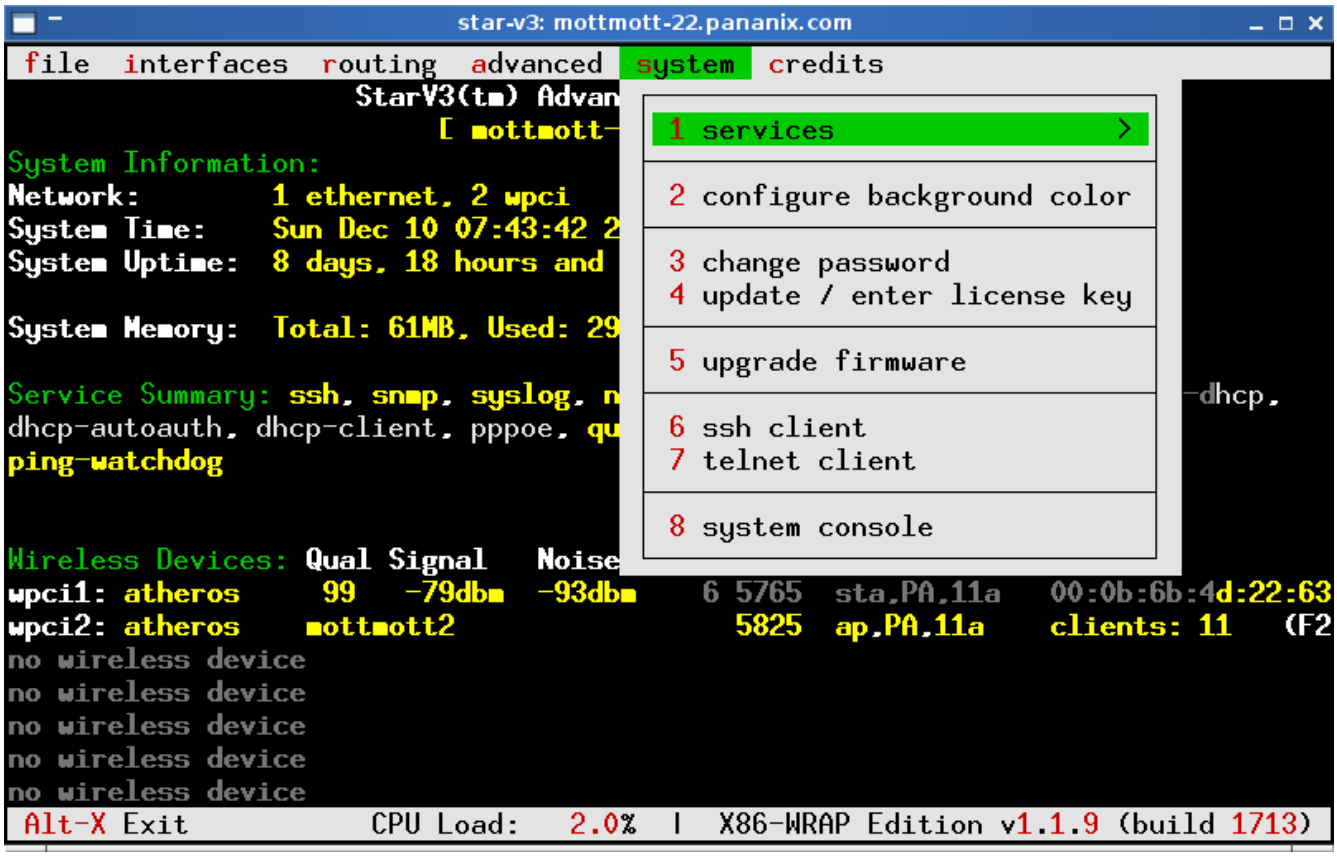
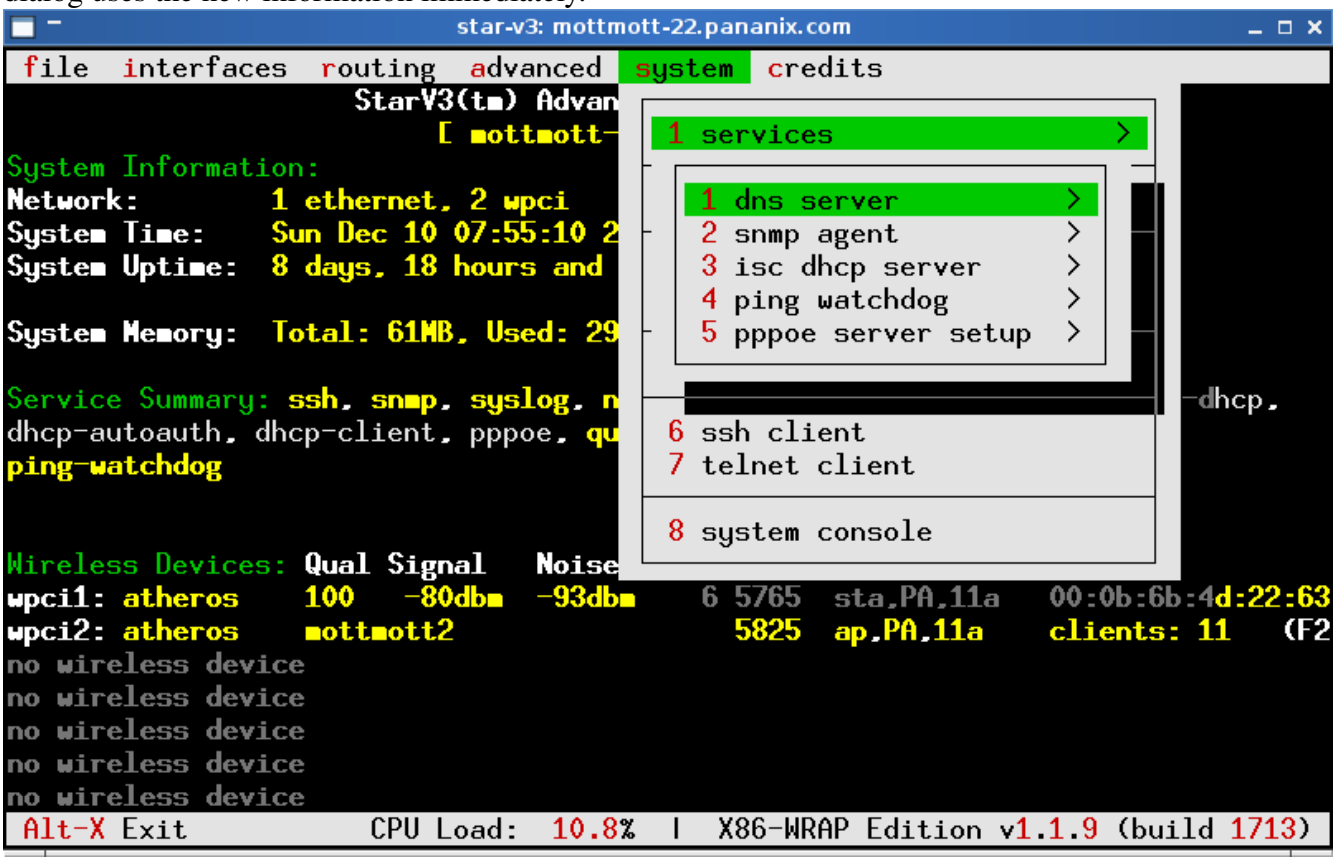

star-v3: mottmott-22.pananix.com
file interfaces routing advanced system credits
StarV3(tm) Advan
[mottmott-
System Information:
Network: 1 ethernet, 2 wpci
System Time: Sun Dec 10 07:43:42 2
System Uptime: 8 days, 18 hours and
System Memory: Total: 61MB, Used: 29
Service Summary: ssh, snmp, syslog, n
dhcp-autoauth, dhcp-client, pppoe, qu
ping-watchdog
-dhcp,
1 services
2 configure background color
3 change password
4 update / enter license key
5 upgrade firmware
6 ssh client
7 telnet client
8 system console
Wireless Devices: Qual Signal Noise
wpci1: atheros 99 -79dbm -93dbm 6 5765 sta,PA,11a 00:0b:6b:4d:22:63
wpci2: atheros mottmott2 5825 ap,PA,11a clients: 11 (F2
no wireless device
no wireless device
no wireless device
no wireless device
no wireless device
Alt-X Exit CPU Load: 2.0% | X86-WRAP Edition v1.1.9 (build 1713)

fig 2: system dropdown

Services

Five services are available for configuration/activation under this menu: DNS cache server, SNMP agent, DHCP server, Ping Watchdog, and PPPOE server (see fig 3). Each service has a configuration box to allow you to choose to restart the daemon on reboot (don't forget to issue a file -> save changes command after making these changes, no file -> activate required). The services also have a service activation option to perform an immediate start/stop/restart of the daemon. You only need to perform a File -> Save to save your setups through reboots. Server start/restart through the service activation dialog uses the new information immediately.


star-v3: mottmott-22.pananix.com
file interfaces routing advanced system credits
StarV3(tm) Advan
[mottmott-
System Information:
Network: 1 ethernet, 2 wpci
System Time: Sun Dec 10 07:55:10 2
System Uptime: 8 days, 18 hours and
System Memory: Total: 61MB, Used: 29
Service Summary: ssh, snmp, syslog, n
dhcp-autoauth, dhcp-client, pppoe, qu
ping-watchdog
Wireless Devices: Qual Signal Noise
wpci1: atheros 100 -80db -93db 6 5765 sta,PA,11a 00:0b:6b:4d:22:63
wpci2: atheros mottmott2 5825 ap,PA,11a clients: 11 (F2
no wireless device
no wireless device
no wireless device
no wireless device
no wireless device
1 services
1 dns server
2 snmp agent
3 isc dhcp server
4 ping watchdog
5 pppoe server setup
6 ssh client
7 telnet client
8 system console
dhcp,
Alt-X Exit CPU Load: 10.8% | X86-WRAP Edition v1.1.9 (build 1713)
fig 3: services dropdown

The DNS server allows you to start a caching name service daemon that any system on your network can use.

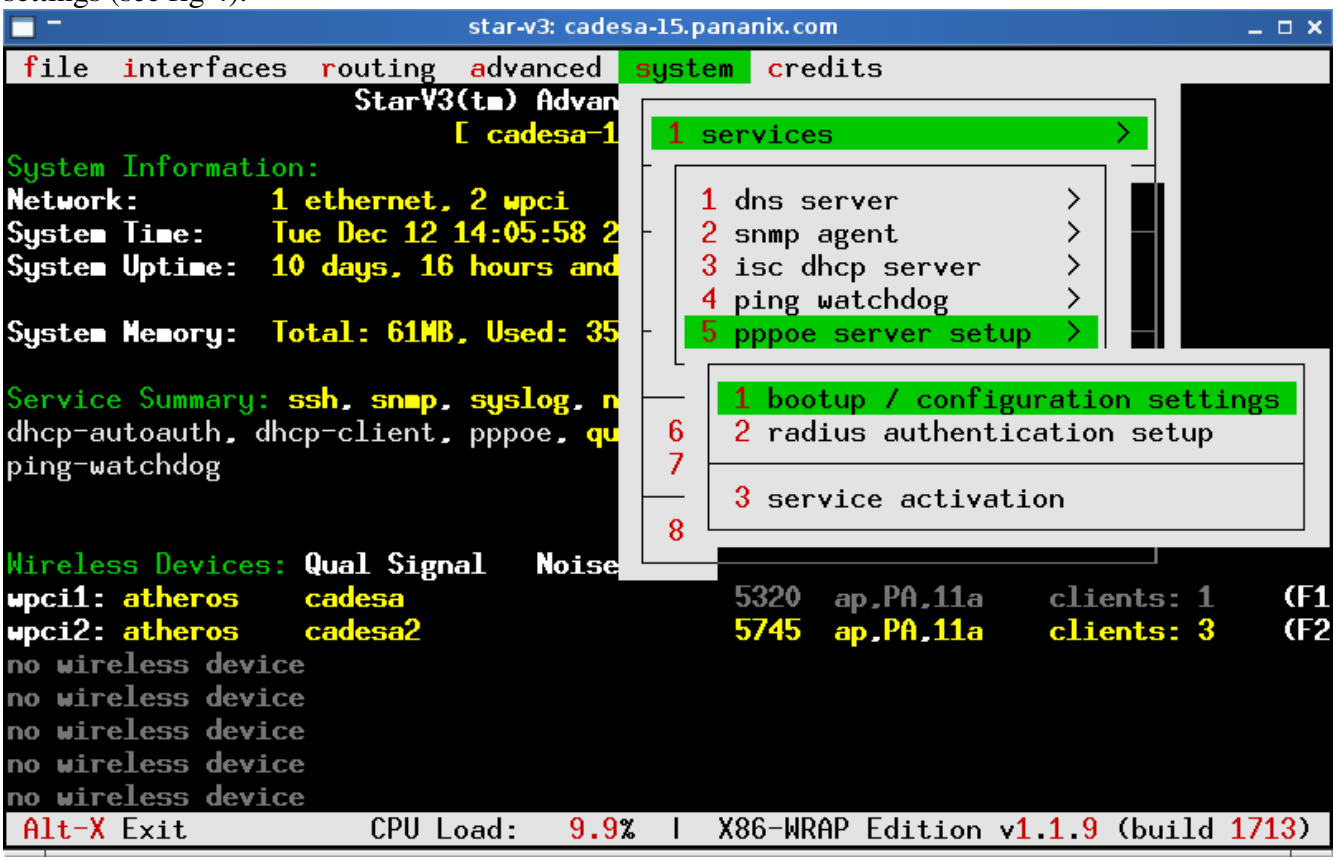
The snmp agent allows you to start/stop the snmp daemon on the system. You can also reconfigure the community name to help keep others from accessing snmp information.

The ISC DHCP server allows you to configure dhcp services for connected clients. To properly configure this service, you should familiarize yourself with ISC's DHCP server version 3. All advanced options are available. The included configuration file will help with a basic setup.

The ping watchdog allows you to force a remote system to reboot if it looses connection with its partner. While working on the system, you might want to disable this to avoid surprises. Don't forget

to reenable it before activating (but not saving) questionable changes. It might save you a long drive. You can also use it if you're making changes that might cause you to lose access to a remote system. Using the watchdog with the file -> activate and selecting “no” when asked to save changes has saved me more than once from a long drive or climbing back up a tower.

The PPPOE server setup allows you to configure the system to access a PPPOE access concentrator to permit PPP connections over your wireless or ethernet links. First, select the bootup/configuration settings (see fig 4).


star-v3: cadesa-15.pananix.com
file interfaces routing advanced system credits
StarV3(tm) Advan
[cadesa-1
System Information:
Network: 1 ethernet, 2 wpci
System Time: Tue Dec 12 14:05:58 2
System Uptime: 10 days, 16 hours and
System Memory: Total: 61MB, Used: 35
Service Summary: ssh, snmp, syslog, n
dhcp-autoauth, dhcp-client, pppoe, qu
ping-watchdog
Wireless Devices: Qual Signal Noise
wpci1: atheros cadesa 5320 ap,PA,11a clients: 1 (F1
wpci2: atheros cadesa2 5745 ap,PA,11a clients: 3 (F2
no wireless device
no wireless device
no wireless device
no wireless device
no wireless device
1 services >
1 dns server >
2 snmp agent >
3 isc dhcp server >
4 ping watchdog >
5 pppoe server setup >
1 bootup / configuration settings
2 radius authentication setup
3 service activation
6
7
8
Alt-X Exit CPU Load: 9.9% | X86-WRAP Edition v1.1.9 (build 1713)
fig 4: PPPOE submenu

The bootup/configuration dialog (see fig 5) will allow you to set up the PPPOE server parameters as well as the IP address range to assign to clients and the authentication methods permitted.

The RADIUS server dialog will allow you to configure the radio to contact the appropriate RADIUS server(s) for authentication and accounting purposes. Changes here will require a restart of the PPPOE daemon and a File -> Save Changes to retain the changes through reboot.

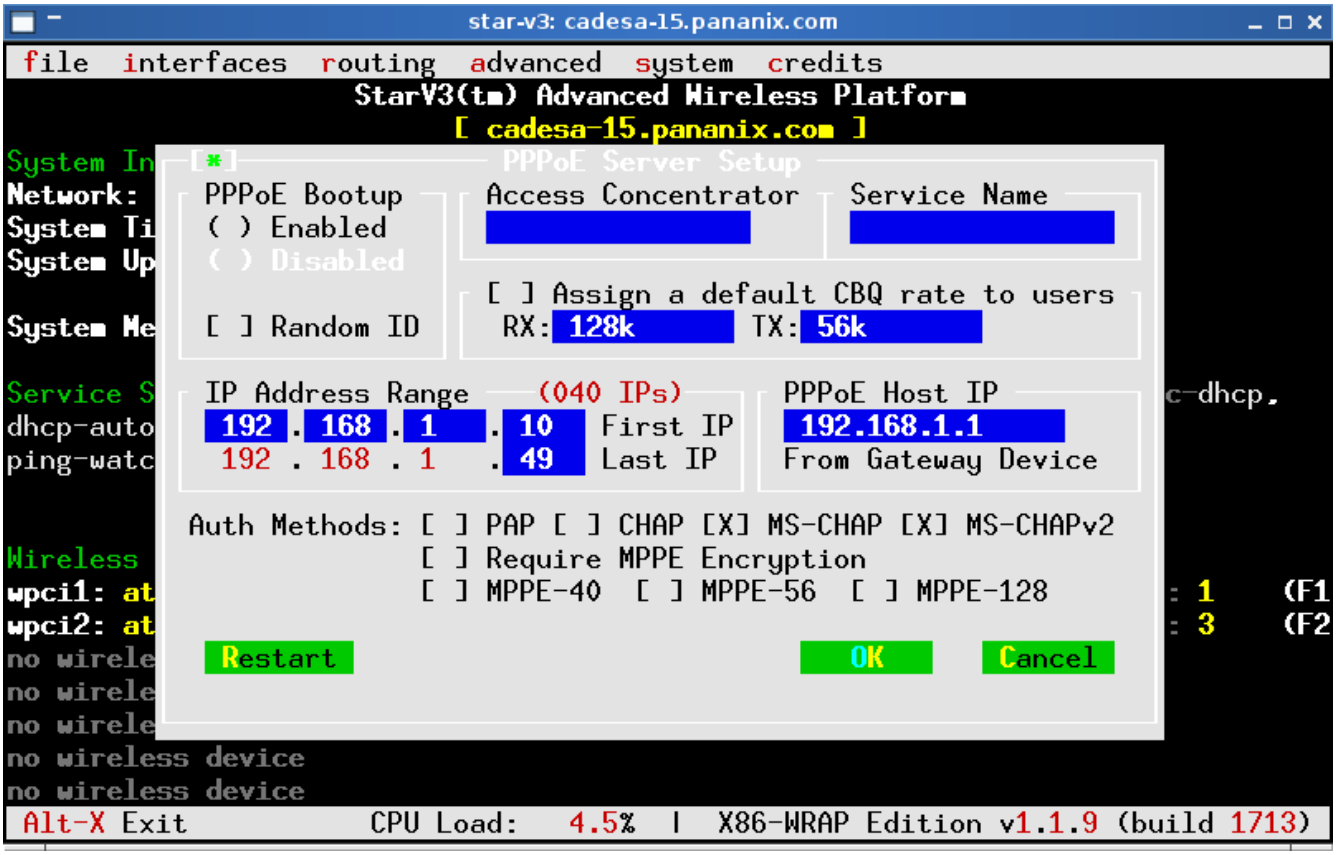

star-v3: cadesa-15.pananix.com
file interfaces routing advanced system credits
StarV3(tm) Advanced Wireless Platform
[cadesa-15.pananix.com]
PPPoE Server Setup
PPPoE Bootup
( ) Enabled
( ) Disabled
[ ] Random ID
Access Concentrator
Service Name
[ ] Assign a default CBQ rate to users
RX: 128k TX: 56k
IP Address Range (040 IPs)
192 . 168 . 1 . 10 First IP
192 . 168 . 1 . 49 Last IP
PPPoE Host IP
192.168.1.1
From Gateway Device
Auth Methods: [ ] PAP [ ] CHAP [X] MS-CHAP [X] MS-CHAPv2
[ ] Require MPPE Encryption
[ ] MPPE-40 [ ] MPPE-56 [ ] MPPE-128
Restart
OK
Cancel
Alt-X Exit
CPU Load: 4.5% | X86-WRAP Edition v1.1.9 (build 1713)

fig 5: PPPOE bootup/configuration dialog

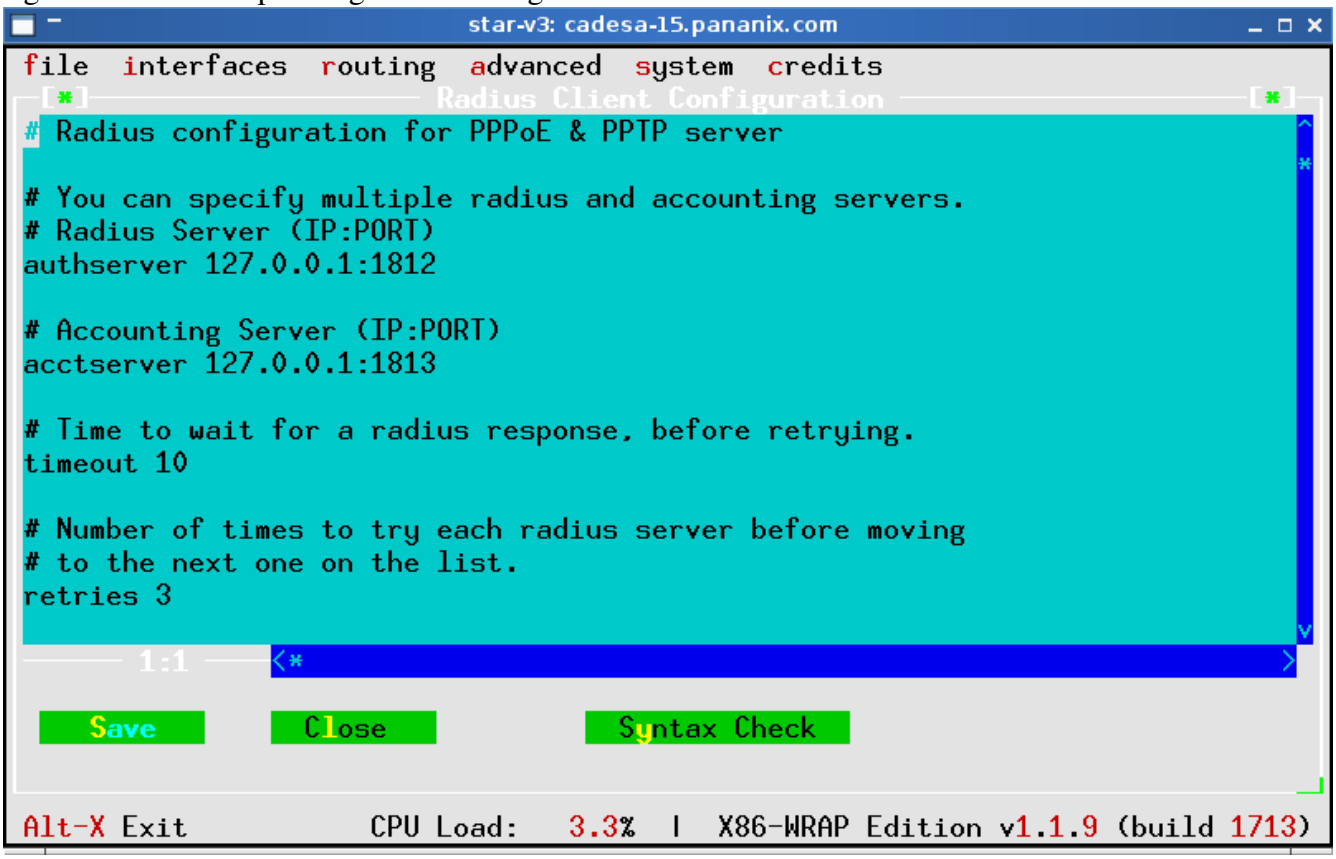

star-v3: cadesa-15.pananix.com
file interfaces routing advanced system credits
Radius Client Configuration
Radius configuration for PPPoE & PPTP server
You can specify multiple radius and accounting servers.
Radius Server (IP:PORT)
authserver 127.0.0.1:1812
Accounting Server (IP:PORT)
acctserver 127.0.0.1:1813
Time to wait for a radius response, before retrying.
timeout 10
Number of times to try each radius server before moving
to the next one on the list.
retries 3
1:1
Save
Close
Syntax Check
Alt-X Exit
CPU Load: 3.3% | X86-WRAP Edition v1.1.9 (build 1713)

fig 6: PPPOE Radius setup

Configure background color

The first option allows you to configure the background color. At this time, your choices are between black and blue. Foreground colors remain the same.

Change password

This option allows you to change the system password. You'll need to know the old password to make the change. The default password for the admin user is 1234. This should be changed before the system is deployed.

Update / Enter License Key

This is where you enter the system key. Remember, the system key is paired to one of the MAC addresses in the machine. If you need to reinstall StarOS from scratch, you'll need the license key to get restore the configuration.

Upgrade firmware

Your StarOS license permits free upgrades to the firmware (first year only on WRAP boards). Upgrade images. are available directly from the StarOS website. Chapter 7 covers how to use starutil to push the upgrade files to the system. Once a new image is on the system, you'll use this option to activate the firmware. Firmware upgrades require a system reboot to take effect.

SSH client

The ssh client provides you the ability to ssh to any other radio or UNIX system running an ssh server.

Telnet client

The telnet client provides an alternative to ssh for antiquated systems that have no ssh access. I shouldn't need to remind you what a bad idea passing usernames and passwords in the clear over radio is.

System Console

A new feature available in V3 is a system console (see fig 7). The system console is designed for those more comfortable with a command line than a menu system.

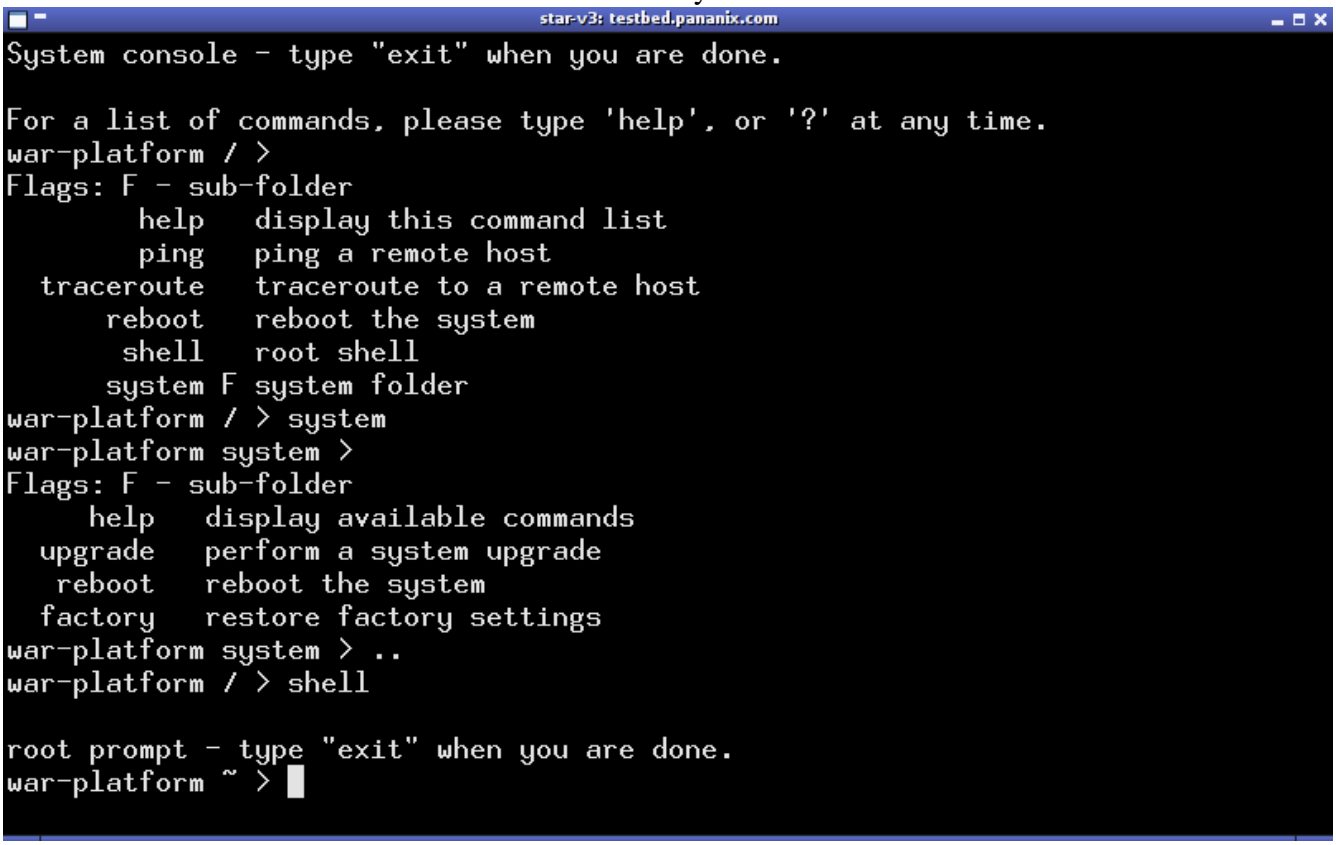

star-v3: testbed.pananix.com
System console - type "exit" when you are done.
For a list of commands, please type 'help', or '?' at any time.
war-platform / >
Flags: F - sub-folder
help display this command list
ping ping a remote host
traceroute traceroute to a remote host
reboot reboot the system
shell root shell
system F system folder
war-platform / > system
war-platform system >
Flags: F - sub-folder
help display available commands
upgrade perform a system upgrade
reboot reboot the system
factory restore factory settings
war-platform system > ..
war-platform / > shell
root prompt - type "exit" when you are done.
war-platform ~ >

fig 7: system console

Upon entering the system console, you'll see the war-platform prompt. Typing "?" will show you what commands are available. This is also true if you enter the system directory by typing "system".

To change directories back up, you can enter "exit" or "..". If you enter the "root" shell, the "?" prompt is not available. Commands that are available include:

- ip
- iperf
- iptables
- ls
- ping
- sh
- ssh
- tcpdump
- telnet
- traceroute

and internal shell commands like cd.

Type "exit" to leave the chroot shell.

It is also possible to enter the system console through the serial port. Presented below are a few comments about the CLI commands available in the shell.

The ip command will permit you to enter via console and check/change the ip address on any system. For those not familiar with ip, just issue the command you want with “show”. Commands may also be abbreviated. Examples:

ip addr sh (will show the ip addresses on the system)

ip ro sh (will show routes)

ip neigh sh (show what the system knows of its neighbors)

You can also issue just “ip” for a usage summary. See the man page for more details.

The iperf command allows you to perform bandwidth tests between two systems. One must run iperf in server mode, the other in client mode. See the man page or usage summary (iperf --help) for more details.

For those advanced administrators who find the firewall interface confining, the iptables command allows them to directly manipulate iptables as well as view iptables statistics. At this time, however, there is no way to save/restore the rules. If, however, the rules are in an external file, the commands may be pasted in the same way the license key is pasted in.

The ssh command acts like a normal ssh client in UNIX, but does not use the .ssh directory or save a list of known hosts. The use of authorized_keys is therefore also unavailable.

By default, the tcpdump and traceroute commands do not do DNS lookups, so the -n option is not available. The tcpdump option to write a file, while available, cannot be used because the filesystem in the radios is not writable by admin.

Chapter 4

The Interfaces Menu

The interfaces menu will allow you to do a wide range of networking setups, including choosing to bridge interfaces, and create virtual distribution systems (VDS) – more on that later. Only the barest of basics was covered in the Getting Started chapter. Much of what is here is new. But first, the basics.

Configuring Interfaces

The Interfaces menu is split into three sections (see fig 1). To keep a logical flow, we'll take these sections out of order starting with the lower section first, since the upper section contains slightly more advanced configurations that generally require more basic things to be configured first.

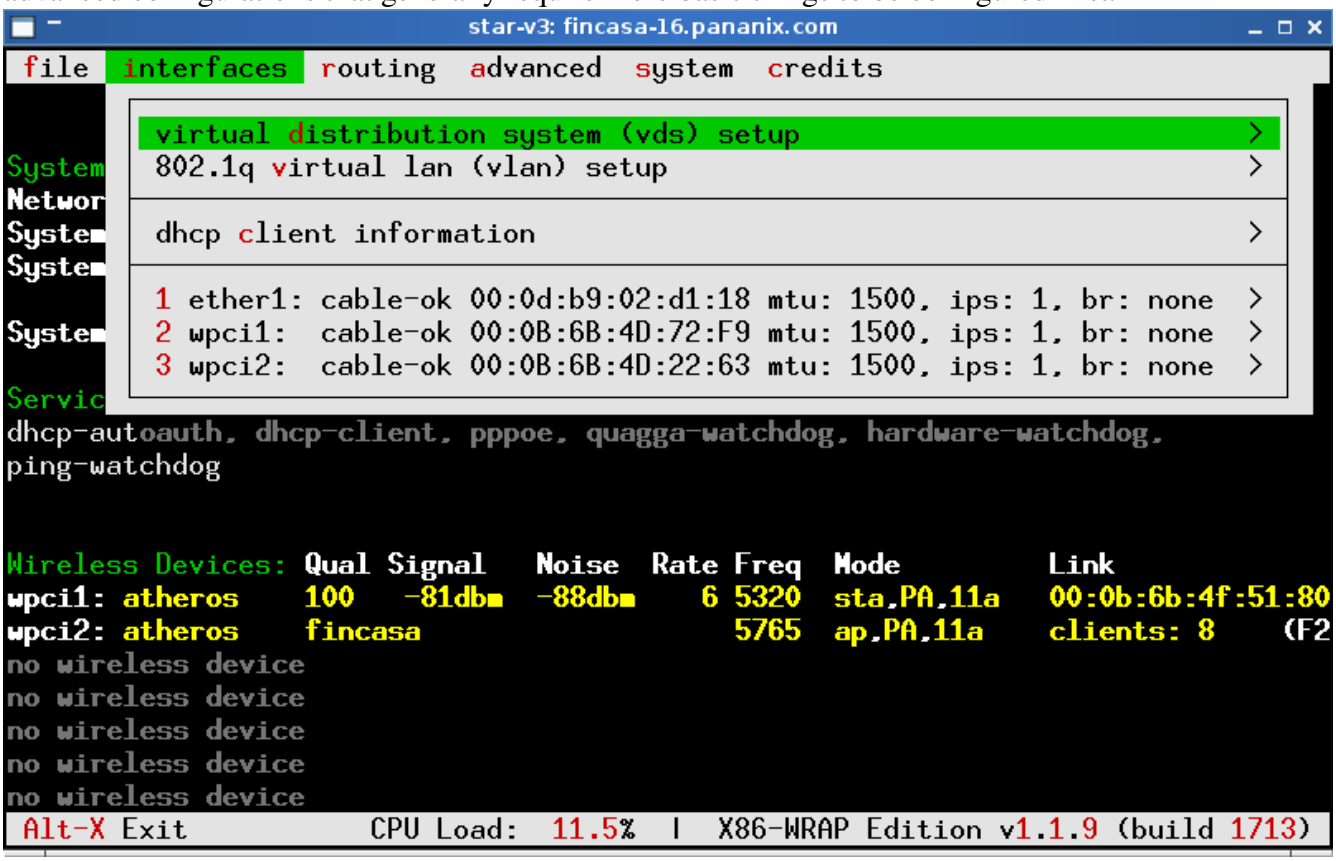

star-v3: fincasa-16.pananix.com
file
interfaces
routing
advanced
system
credits
virtual distribution system (vds) setup
802.1q virtual lan (vlan) setup
dhcp client information
1 ether1: cable-ok 00:0d:b9:02:d1:18 mtu: 1500, ips: 1, br: none
2 wpci1: cable-ok 00:0B:6B:4D:72:F9 mtu: 1500, ips: 1, br: none
3 wpci2: cable-ok 00:0B:6B:4D:22:63 mtu: 1500, ips: 1, br: none
dhcp-autoauth, dhcp-client, pppoe, quagga-watchdog, hardware-watchdog,
ping-watchdog
Wireless Devices: Qual Signal Noise Rate Freq Mode Link
wpci1: atheros 100 -81db -88db 6 5320 sta,PA,11a 00:0b:6b:4f:51:80
wpci2: atheros fincasa 5765 ap,PA,11a clients: 8
no wireless device
no wireless device
no wireless device
no wireless device
no wireless device
Alt-X Exit
CPU Load: 11.5% | X86-WRAP Edition v1.1.9 (build 1713)

fig 1: interfaces menu

Ether and Wireless Cards

Each physical device you have in your system will have a line in the interfaces menu (see fig 1). This line contains a summary of information about that device. Following the device name (used to identify the device in scripts in the advanced menu) is the devices MAC address, the MTU, number of configured IPs, and the bridge number to which a device belongs. Note that, while the wireless devices here are numbered starting with 1, if you use the system console, you'll find the devices numbered

beginning with 0 in the usual UNIX custom.

Device submenus

Each physical device has a submenu to provide access to various configuration items. (see fig 2).

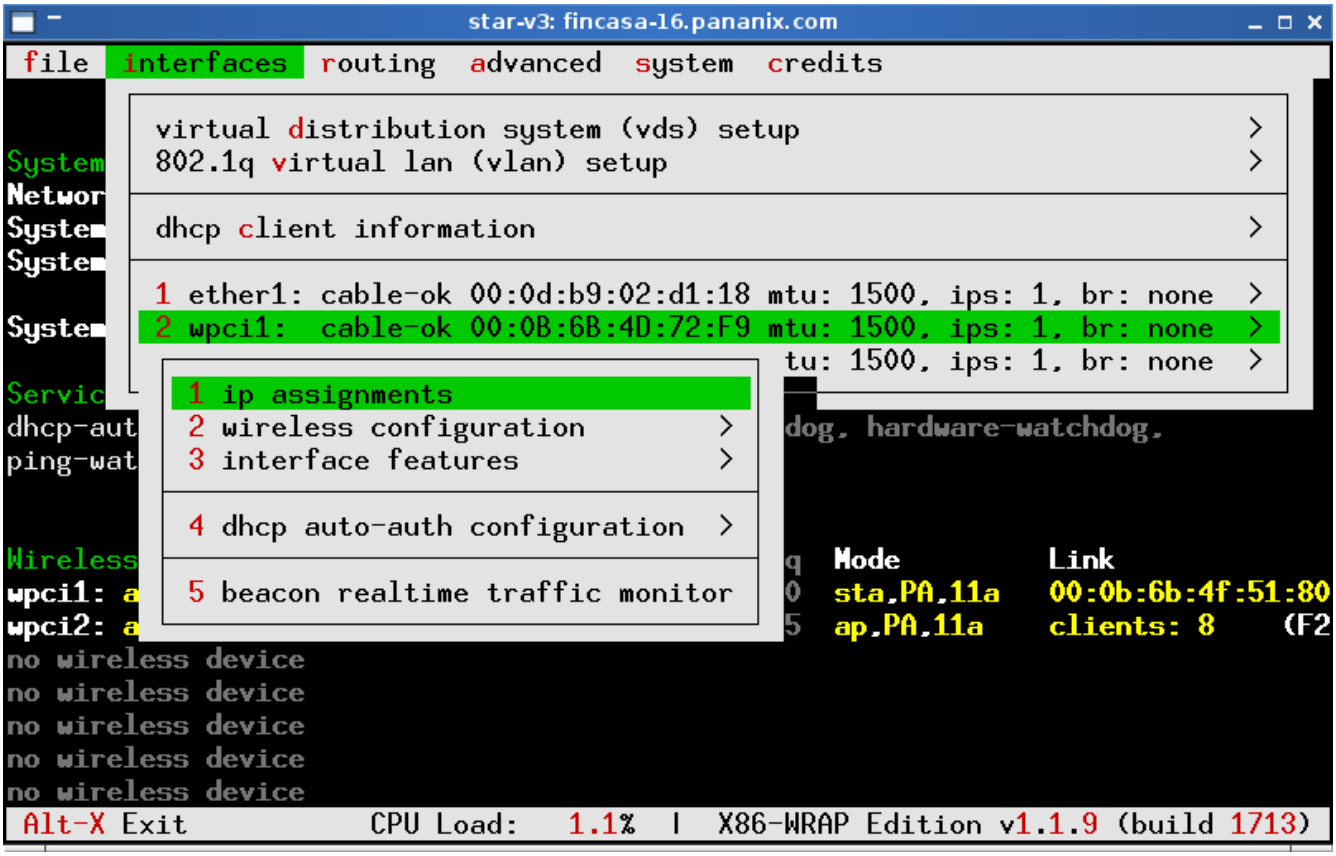


fig 2: physical devices submenu

IP assignments

Most systems will require at least one of your devices to have an IP address. While it is possible for a bridged system to run without an IP address, access to the system would then only be possible via the serial port (if available). Routed systems require an IP address on a different subnet on each interface.

Selecting IP assignments presents the box shown in fig 3.

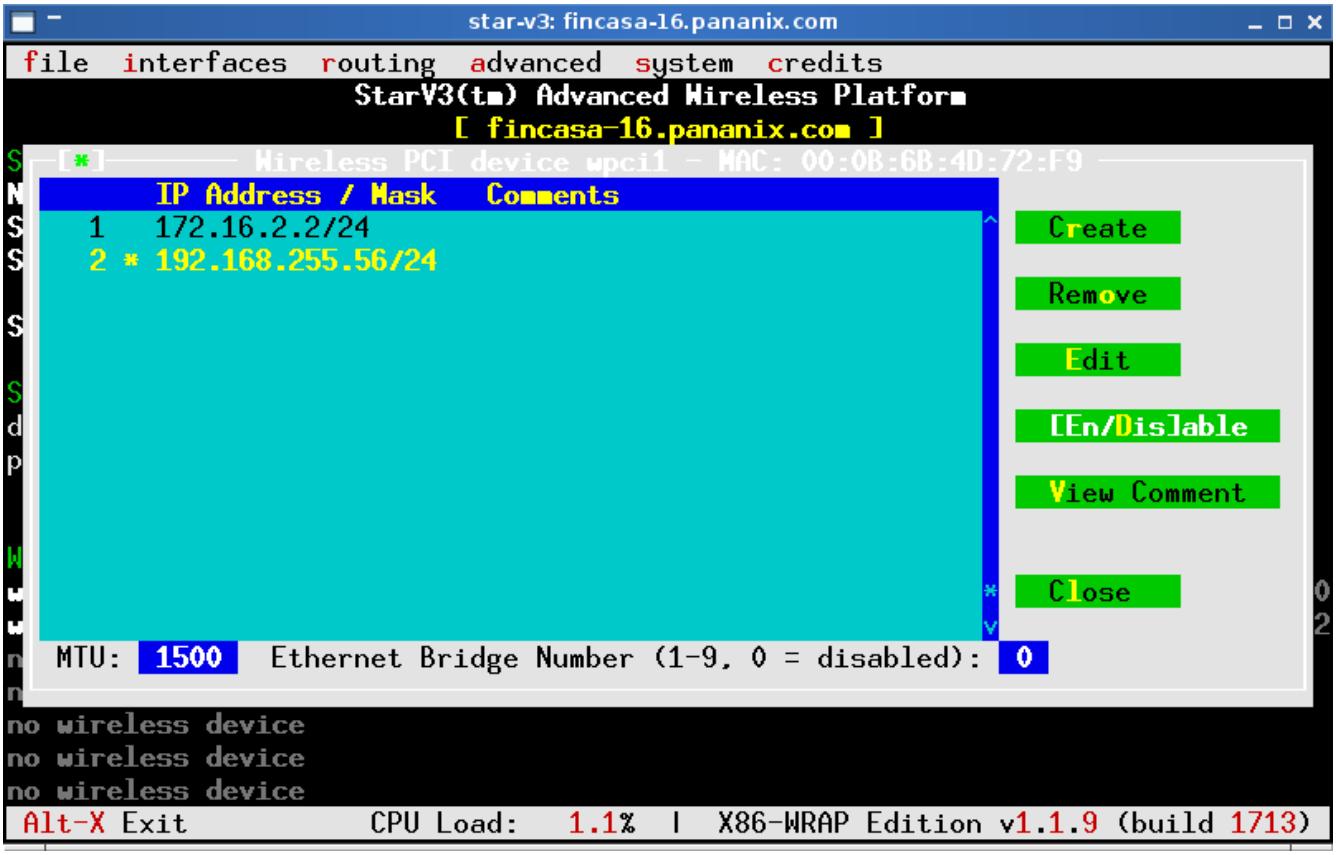


fig 3: IP assignments box

The main box shows any IPs assigned to the interface with the subnet mask in VLSM (CIDR) notation, followed by the beginning of any comment you may have for that card. If no IPs are assigned to an interface, this box will have the notation <empty>. IPs that are disabled are shown by an asterisk in front of the IP. To perform a function on an IP, select that line then the function you want to perform to the right.

The Create selection item will provide a box allowing you to designate an IP, netmask (in dotted decimal notation form), and an optional comment.

The Remove selection removes a highlighted IP.

The Edit selection provides a box similar to the Create box, but with the current information filled in.

The [En/Dis]able button allows you to enable or disable the selected IP.

The View Comment line shows a box where you can read any comment associated with a particular IP.

The Close button returns you to the main menu.

Below the main window are two other configuration options, the MTU and Ethernet Bridge Number. The MTU box will default to 1500. While there are circumstances under which you may need to modify this number downwards (such as using both VLAN and VPN, or when connected to other devices requiring a lower MTU), in general, the default should be used. The Ethernet Bridge Number allows you to bridge two or more devices together. Up to 9 bridges may be created (although you'll

need at least 18 devices to create this many bridges). Bridge number 0 disables bridging for the device.

Use either Close or <ESC> to leave the box and return to the main menu. In either case, all changes remain, but must be activated using the File->Activate menu to take effect. Any changes not saved will not remain through a reboot.

Wireless Configuration

The wireless configuration menu is now part of the interface menu to which it pertains (see fig 4). Ethernet cards have a corresponding “Ethernet Configuration” submenu containing an ethernet link settings selection (see fig ?) in the Ethernet Configuration section below.

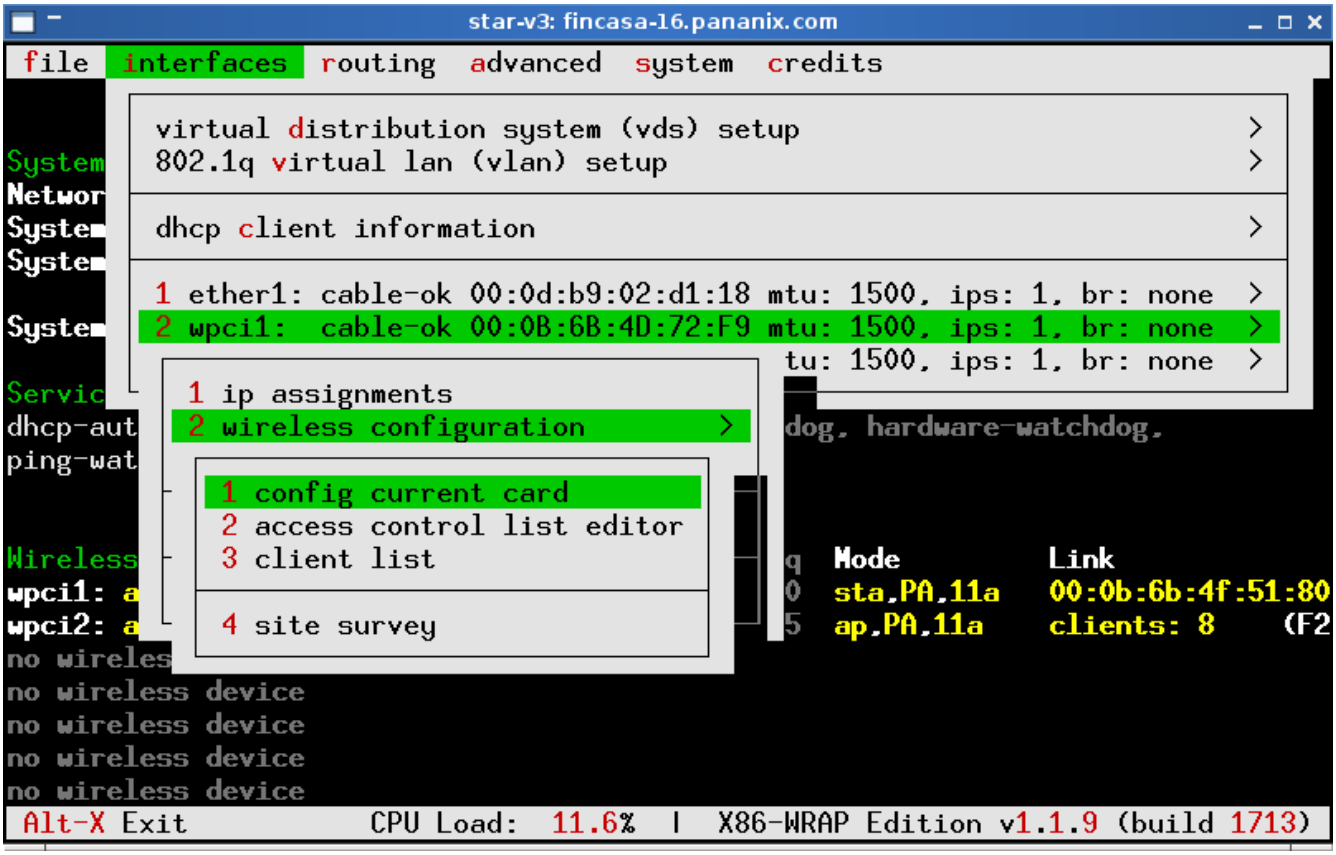


fig 4: wireless configuration

Config current card

In this menu you'll do everything to configure the radio card (see fig 5). This menu was covered briefly in the Quick Start chapter, but will be expanded here. This text will only cover the Atheros

Enable

StarOS V3 has an option to disable a network card installed in a system for whatever reason. If you want to use the card, you must ensure this is enabled. If disabled, under Wireless devices on the main screen, you will see “card is disabled.”

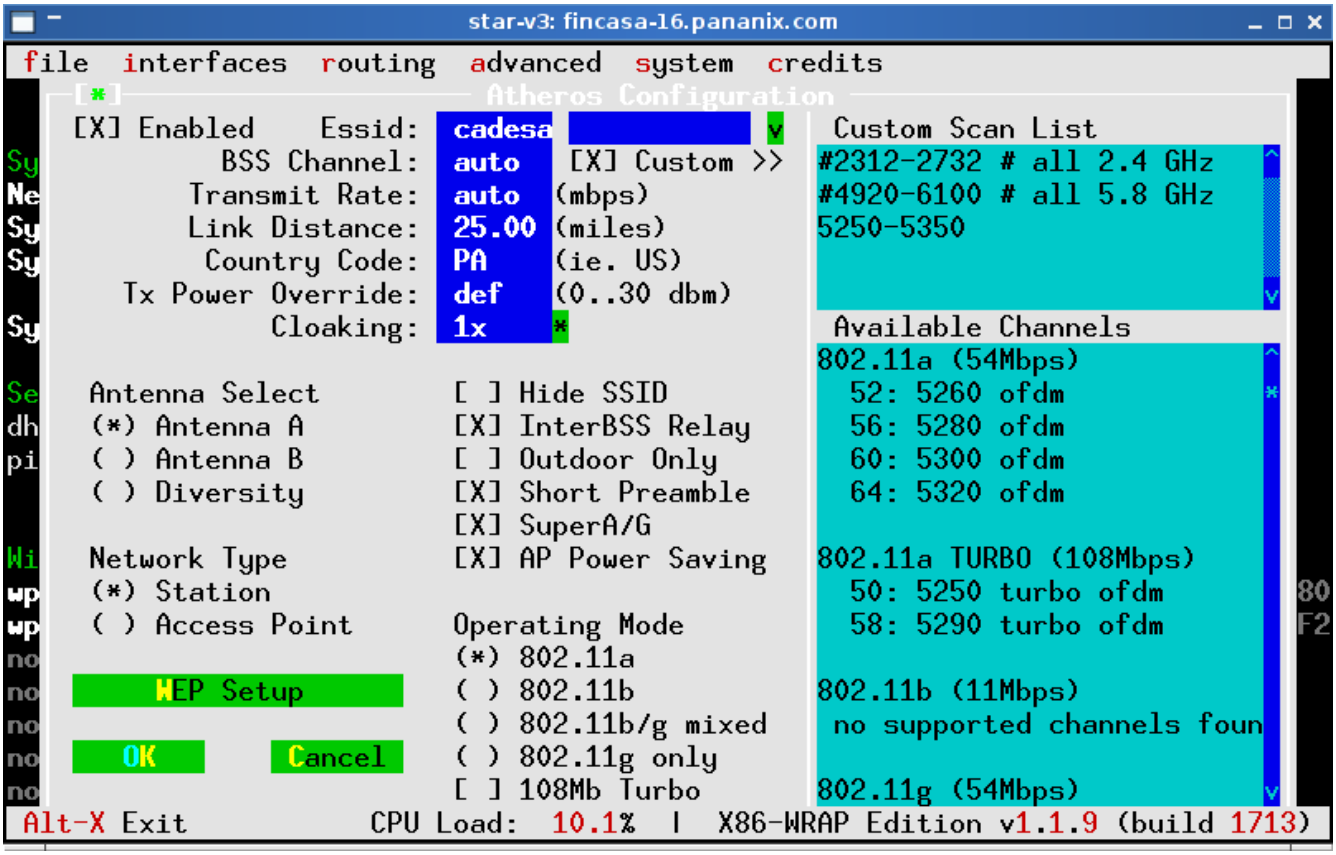


fig 5: wireless card configuration screen

ESSID

This is where you'll put your network name. ESSID stands for Extended Service Set Identification, ESSID. You have space for a 16 digit alphanumeric sequence, but I suggest you don't extend it that far. Choose a unique name that is representative of your system, either its location or function, that is short. After all, you'll have to type it into all your client radios (or select it when the signal is seen).

BSS Channel

The base station system channel. This box is only required if the system will function as an Access Point. When programmed as a station (client), the value in this box is ignored. You can put either a 1, 2, or 3 digit channel number or a 4 digit frequency. If you input an invalid value, the card will ignore it and default to the lowest frequency available based on the country code and if activated, the custom channel list (which will be a subset of the country code channels available). Note that, 802.11a and 802.11a super frequencies do not coincide.

Custom Checkbox and Scan List

The Custom checkbox can be used to force the client to only scan certain channels rather than all the channels in the available channels list for the particular mode you're scanning.

The Custom Scan List will also be used in AP mode and limit what you will see in the available channels list.

The Custom Scan list can be edited. A # sign will act as a remark. You may enter one frequency per line to only scan certain frequencies or put two hyphen separated frequencies as shown in the Custom Scan List to scan a range, one range per line.

Transmit Rate (mbps)

The transmit rate refers to the connection speed you want the radios to connect at. The default is auto, and the cards will autobaud to the best speed depending on conditions (noise, SNR, etc.). You can preset a speed to lock systems in. This will prevent distant (weak) stations from slowing down traffic and help keep things flowing. You must put a valid speed for your selected operating mode. Modes and speeds are listed for your convenience:

802.11b	*802.11a/g*	*802.11a/g turbo*
1	6	12
2	9	18
5.5	12	24
11	18	36
	24	48
	36	72
	48	96
	54	108

Link distance (0..35 miles)

The link distance in miles is extrapolated to a delay for acknowledgment packets. Putting too low a value here will result in a radio connect, but no IP traffic will flow. Putting the smallest possible number here will purportedly make your link faster. While this is true for extreme values, it will mostly help you make or break a connection with distant stations. Set this to a value slightly higher than farthest expected client station. The default (def) is a fairly small distance, approx 300 feet, generally too small for outdoor networks.

Country code

The default country code (n/a) will provide you a representative list of channels/frequencies. If you are in a country that is programmed into the radio card, select that country (see Appendix A). If you change the country code, you'll need to go to the File menu and select Activate then return to this menu. The available channels/frequencies will be listed in a box in the right third of the wireless menu. Select your channel/frequency from this list for your chosen operating mode.

Tx Power Override (0..30 dbm)

This feature allows you to select the precise amount of power you want to send out the card's antenna

connector. This facilitates running your AP or client at the optimum power setting without exceeding EIRP maximums for your area. A word of caution: setting the dbm to 0 will not provide 1mW output power as you might expect, but will set the card to its default power setting. The default is normally 15dbm (generally between 30-35mW) for most cards. Also, not all cards are capable of running at 1W (30 dbm). Check your cards specifications for default and maximum power. Maximum power may depend on operating mode/frequency.

Cloaking

Cloaking is used to signify what some HAM operators might call a filter. In this case, the filter will narrow the bandwidth used. The menu will allow you to set values of 1, 2, or 4. Divide the normal frequency bandwidth by the number chosen. This will allow you to maximize frequency usage on a tower in the 2.4GHz range by allowing each channel to use less bandwidth. Where before, 4 channels in the 802.11b (2.4GHz) band could be used without overlap, now all available frequencies can be used without significant adjacent channel interference. In the 5GHz range, this will provide you with more non-overlapping channels. That is, at cloaking value 1, available frequencies may include 5745, 5765, 5785, etc. At cloaking value 2, values will include 5745, 5755, 5765, 5775, etc., and at cloaking value 4, this list will include 5745, 5750, 5755, 5760, 5765, etc.

When cloaking is used, your throughput at any given speed will be half or quarter the throughput (at cloaking values of 2 or 4 respectively) with no cloaking (cloaking value 1). You can compensate by forcing the system to only connect at higher transmit rates which will require better SNR. You may also be able to slip between two interfering stations and get a better connection using cloaking which may make up for its use via better throughput. The only way to know is experiment.

Antenna Select

Choose the antenna connector your antenna is connected to. In general, you'll choose antenna A, which is usually the connector in the extreme corner of the card. Antenna B may be marked AUX (auxiliary). Diversity is the newer spatial diversity antennas designed to improve sensitivity without increasing power output. These antennas are recognizable from the dual connectors. Choosing Diversity will make both antenna connectors active. A note about spacial diversity antennas: these antennas have two connectors because inside they are two antennas. However, they are carefully impedance matched, and the cables used to connect to these should be matched for best performance. Do not connect two unmatched antennas to one card as performance will be degraded (and at least one antenna may output more than the legal power).

Hide SSID

Selecting this box will tell the AP not to broadcast its ESSID. The 802.11 specification calls for the AP to announce itself. However, private networks will often choose not to. A number of wireless network operators mistakenly implement this as their only security. While this may help, it does not replace proper security and authentication methods.

InterBSS Relay

If you want clients to be able to communicate between each other when connected to the same AP, you'll need to enable this setting. When checked, clients can talk to other clients. When unchecked, client-to-client traffic is suppressed.

Outdoor Only

When selected, any frequencies that, by regulation (according to the chosen country code) can only output reduced power levels, are considered indoor frequencies and will be removed from the Available Channels list. Deselecting this will return the channels to use. You will need to select File->Activate to see the desired results.

Short Preamble

Some older cards, principally 802.11b cards, only understand the original long preamble sent at the beginning of wireless management frames. If all your clients are newer cards that can understand the short preamble, you'll want this enabled. By default, it is enabled.

Super A/G

Super A/G encapsulates some of the algorithms meant to speed up communications. Check this if you wish to use bursting, compression, and fast frames.

AP Power Saving Mode

AP power saving mode powers down the card when no clients are requesting access. This can help save power at sites using solar cells.

Network Type

Here, you must select either Access Point (AP) or Station (client) mode.

Operating Mode

You can select between 802.11a (5.8GHz OFDM), 802.11b (2.4GHz DSSS), mixed 802.11b/g (2.4GHz), 802.11g only (no switching for 802.11b only clients) frequencies for your AP. Selecting one of the operating modes for a client will limit the scan. This will result in the client finding the AP faster. Selecting 108Mb Turbo will allow your radio to transmit at twice the rate. Note that, this setting will require a higher SNR to achieve these speeds. If you couldn't connect consistently at 54Mbs, you won't get 108Mbs, but you still may get more speed than without turbo.

Available Channels Window

This window shows the channel and frequencies available for use depending on what you've entered in the country code setting above. These will show the frequencies permitted in that country, but after entering the country code you must first save and activate your changes.

WEP Security submenu

WEP (Wireless Encryption Protocol) has been shown to have serious defects. But using it is definitely better than not. Combined with other authentication mechanisms, WEP helps keep your data private. But if you need real data security, you'll be better off building encrypted tunnels. The VDS menu under interfaces can do this. But if you need many tunnels, consider building them through your radios rather than between them.

Meanwhile, select the best WEP encryption you can. You'll have to use 104 bit encryption with Microsoft radio clients. Otherwise, choose 128. The 40 bit is only for legacy equipment and is nearly worthless today. Even 128 can be broken once enough traffic has passed.

The pass phrase can be used to generate the same keys in all systems.

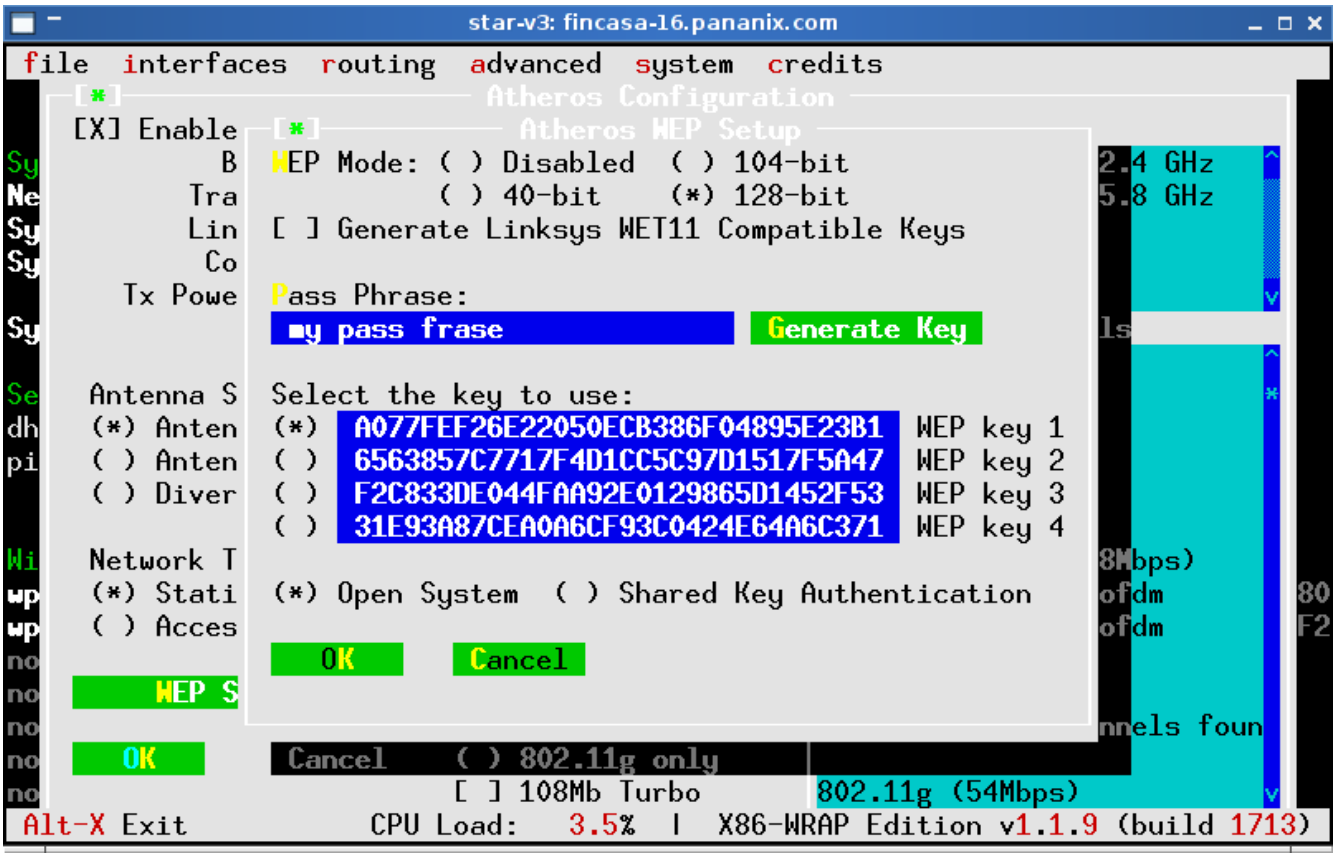
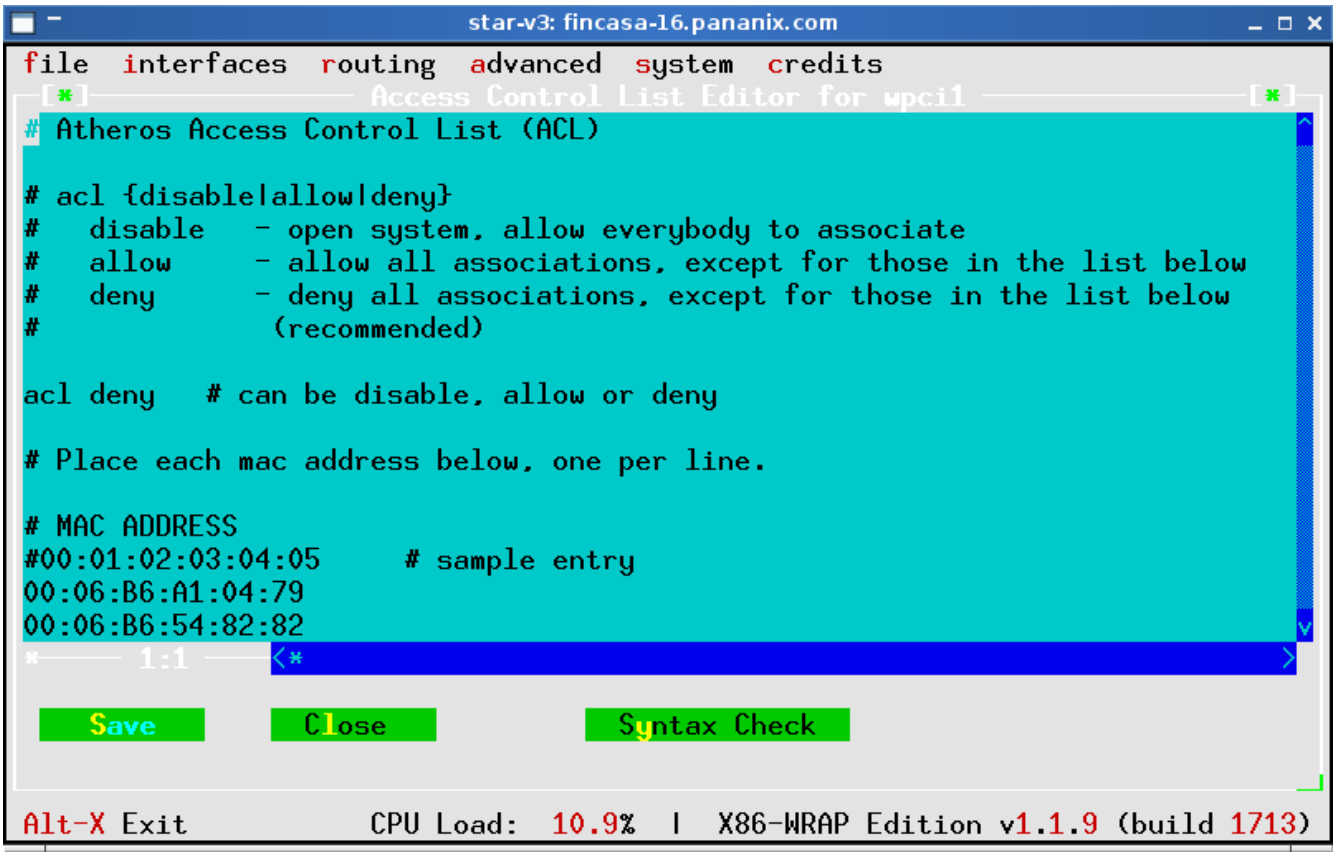


fig 6: WEP setup box

Access Control List Editor

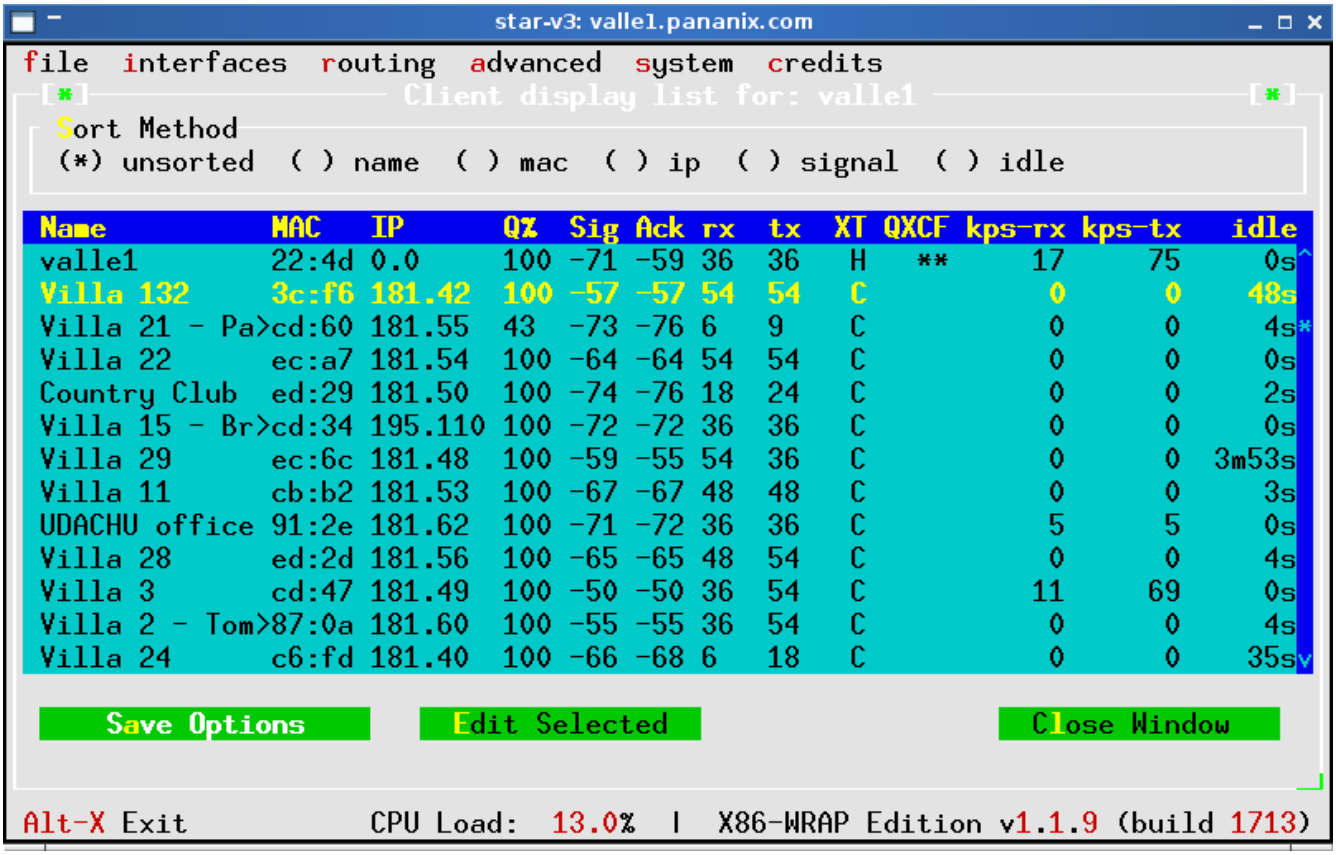
The access control list editor allows you to permit or deny access based on the MAC address reported by the client. By default, the ACL is disabled. But you can easily change this to one of allow or deny. If set to allow, it sets up a policy of allow and listed MAC addresses are blacklisted. If set to policy deny, then all connections except those explicitly permitted are denied (see fig 7).

Note that MAC address spoofing can bypass your access controls. An ACL isn't foolproof, but adds yet another layer of control.


star-v3: fincasa-16.pananix.com
file interfaces routing advanced system credits
Access Control List Editor for wpci1
Atheros Access Control List (ACL)
acl {disable|allow|deny}
disable   - open system, allow everybody to associate
allow   - allow all associations, except for those in the list below
deny   - deny all associations, except for those in the list below
(recommended)
acl deny   # can be disable, allow or deny
Place each mac address below, one per line.
MAC ADDRESS
#00:01:02:03:04:05   # sample entry
00:06:B6:A1:04:79
00:06:B6:54:82:82
1:1
Save
Close
Syntax Check
Alt-X Exit
CPU Load: 10.9% | X86-WRAP Edition v1.1.9 (build 1713)
fig 7: Access Control List

Client List

The client list, shown on the AP as the client display list (see fig 8) shows details of all clients as well as the state of the AP itself.


star-v3: valle1.pananix.com
file interfaces routing advanced system credits
Client display list for: valle1
Sort Method
(*) unsorted ( ) name ( ) mac ( ) ip ( ) signal ( ) idle
Name MAC IP Q% Sig Ack rx tx XT QXCF kps-rx kps-tx idle
valle1 22:4d 0.0 100 -71 -59 36 36 H ** 17 75 0s
Villa 132 3c:f6 181.42 100 -57 -57 54 54 C 0 0 48s
Villa 21 - Pa>cd:60 181.55 43 -73 -76 6 9 C 0 0 4s
Villa 22 ec:a7 181.54 100 -64 -64 54 54 C 0 0 0s
Country Club ed:29 181.50 100 -74 -76 18 24 C 0 0 2s
Villa 15 - Br>cd:34 195.110 100 -72 -72 36 36 C 0 0 0s
Villa 29 ec:6c 181.48 100 -59 -55 54 36 C 0 0 3m53s
Villa 11 cb:b2 181.53 100 -67 -67 48 48 C 0 0 3s
UDACHU office 91:2e 181.62 100 -71 -72 36 36 C 5 5 0s
Villa 28 ed:2d 181.56 100 -65 -65 48 54 C 0 0 4s
Villa 3 cd:47 181.49 100 -50 -50 36 54 C 11 69 0s
Villa 2 - Tom>87:0a 181.60 100 -55 -55 36 54 C 0 0 4s
Villa 24 c6:fd 181.40 100 -66 -68 6 18 C 0 0 35s
Save Options
Edit Selected
Close Window
Alt-X Exit
CPU Load: 13.0% | X86-WRAP Edition v1.1.9 (build 1713)
fig 8: Association List/Client display list

The first line shows the network name (unless changed). Subsequent lines show client names if input. This is followed by the MAC address (last two words only, the first four are suppressed in the interests of space). Then comes the last IP seen passing through the AP from that client, again, only the last two octets are shown to conserve space.

The next several fields describe the connection itself. The Q% basically shows percent of first time transmits that made it through. As the connection quality drops off (for whatever reason), the percentage of first transmit successful packets will decrease. The next number is the link signal. The Ack number is the last ack signal strength. This is followed by the receive (rx) and transmit (tx) wireless connection speeds.

The next two fields, XT, show whether the client is using XR (Atheros eXtended Range) and the connection type. All systems should have a first line with H, the host itself. If it is associated with another system, subsequent lines will show one of C for client, A for AP, W for WDS, or N for disassociated connection.

The next four fields, QXCF. show whether QOS is supported, XR is supported, compression is being used, and Fast Frames is being used.

The next two fields, show in fig 2 as kps-rx and kps-tx show current receive and transmit throughput with the associated client in kilobits per second.

Finally, the idle time. This is the time since last traffic was passed.

Site Survey

The site survey, greyed out when in AP mode (because this really does only make sense in station mode), shows sites the system knows about because it has seen them (see fig 9).

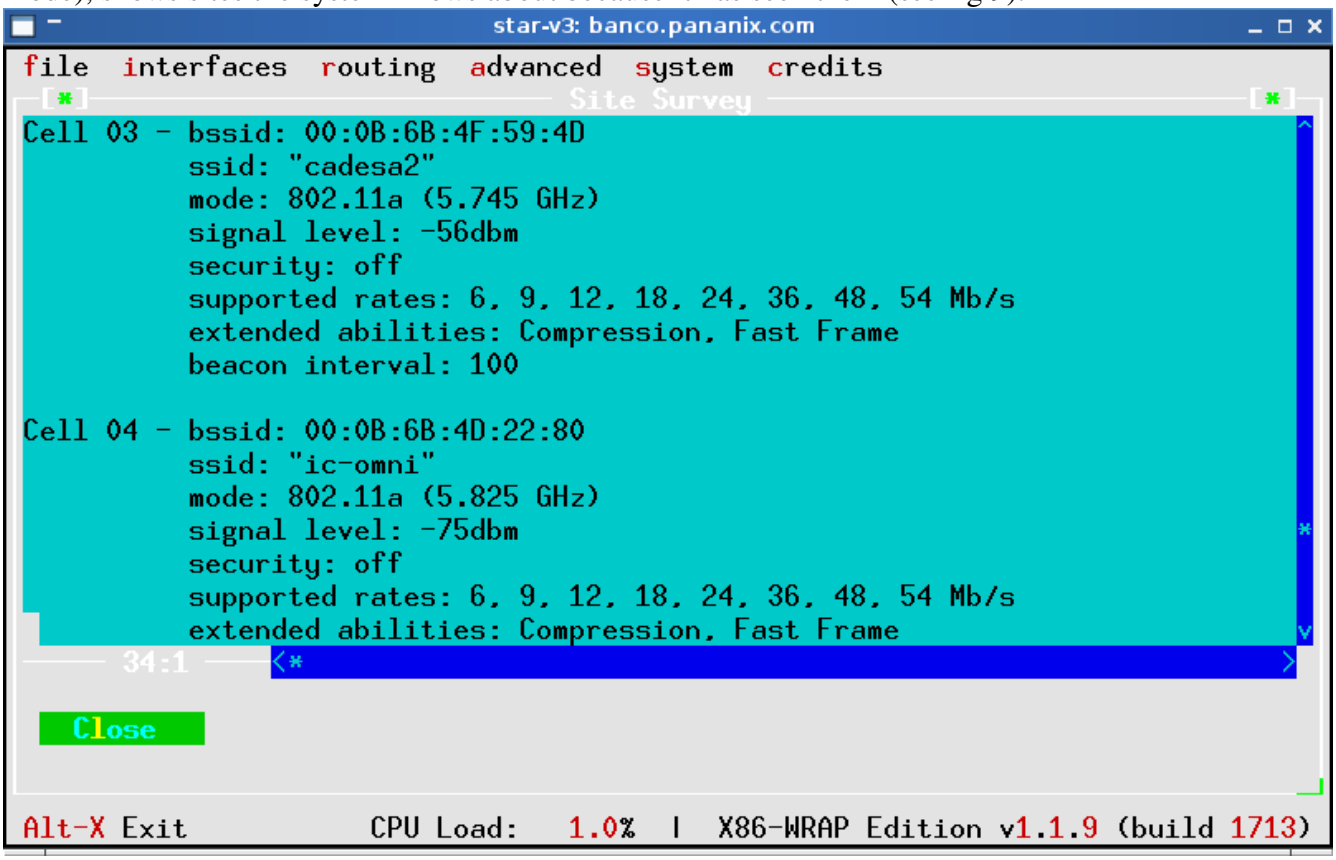

star-v3: banco.pananix.com
file interfaces routing advanced system credits
Site Survey
Cell 03 - bssid: 00:0B:6B:4F:59:4D
ssid: "cadesa2"
mode: 802.11a (5.745 GHz)
signal level: -56dbm
security: off
supported rates: 6, 9, 12, 18, 24, 36, 48, 54 Mb/s
extended abilities: Compression, Fast Frame
beacon interval: 100
Cell 04 - bssid: 00:0B:6B:4D:22:80
ssid: "ic-omni"
mode: 802.11a (5.825 GHz)
signal level: -75dbm
security: off
supported rates: 6, 9, 12, 18, 24, 36, 48, 54 Mb/s
extended abilities: Compression, Fast Frame
34:1
Close
Alt-X Exit
CPU Load: 1.0% | X86-WRAP Edition v1.1.9 (build 1713)

fig 9: site survey

Where sites do not have an ssid showing (ssid: “”), it is because that APs essid is hidden. The rest of the information shown should be self-explanatory.

Ethernet Configurations

Like the wireless cards, the ethernet cards also have ethernet settings peculiar to them, which may be accessed and changed via the Interfaces -> ethernet# -> ethernet configuration link (see fig 10)

Ethernet Link Settings

This will bring up a dialog box showing the current mode of the ethernet port, and options to change it. By default, the ethernet port will do autonegotiation. This can be turned off, and the speed (10Mb or 100Mb) may be specified, as well as full duplex or not.

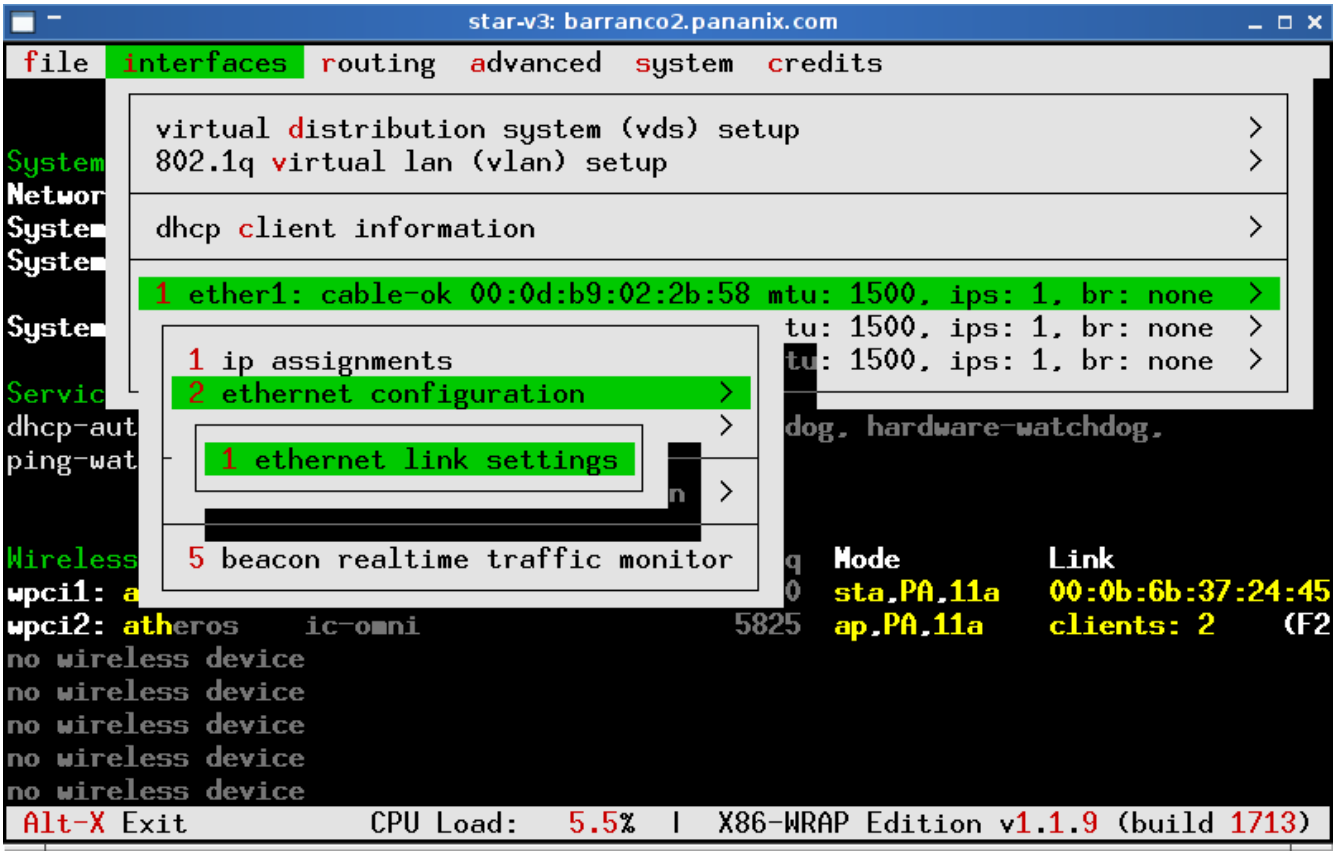


fig 10: ethernet link settings

Interface Features

Any given interface currently has three features that my be activated (see fig 11).

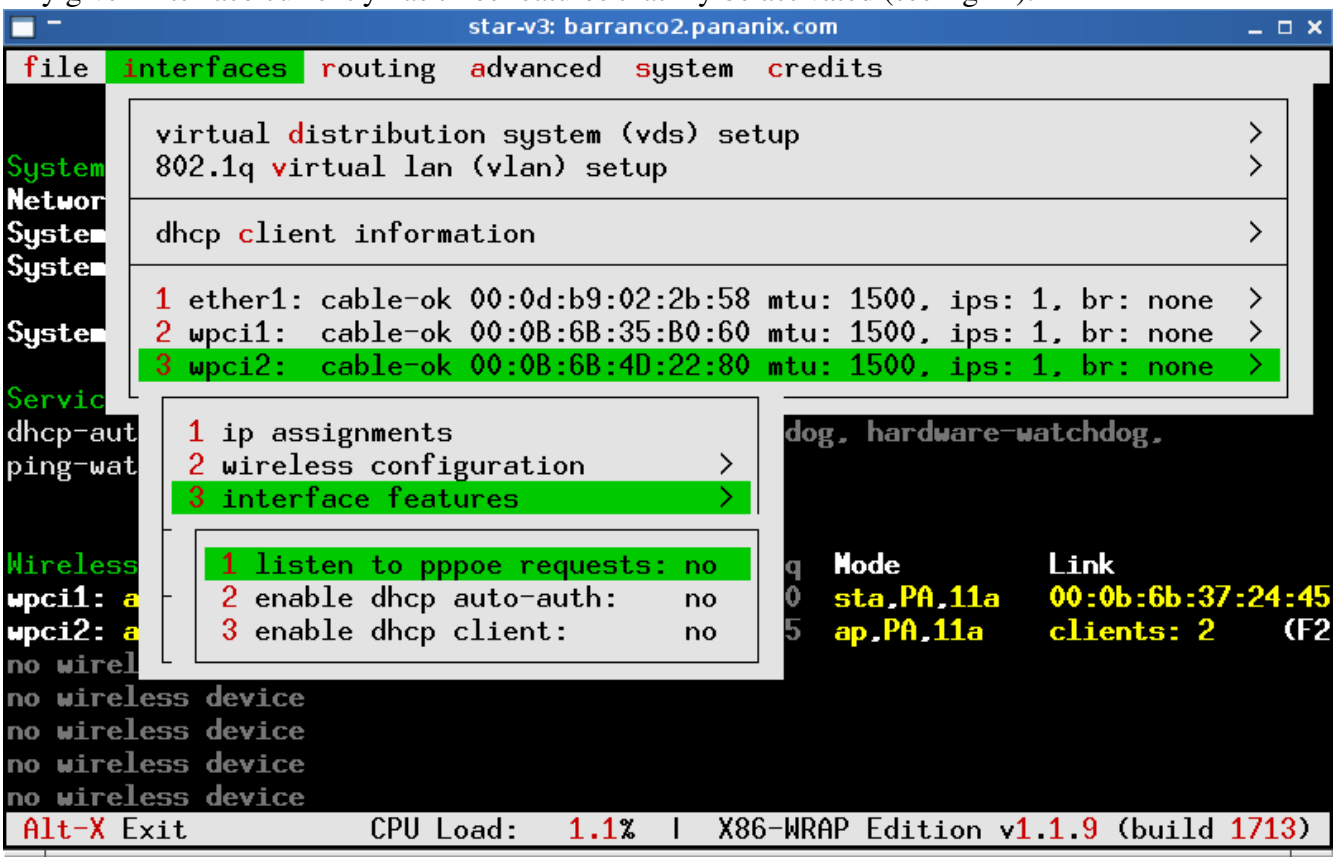


fig 11: interface features

If the System -> Service -> PPPOE Server setup is used and you want to allow PPPOE connections on this interface, then this should be turned on. When the status of a particular interface is changed from off to on or vice versa, the PPPOE server must be restarted.

The dhcp auto-auth should be activated when users authenticate via RADIUS (such as when the system is used as a hotspot) and get their IP address via DHCP. This allows the RADIUS server to manage IP address assignments following authentication. If you use the regular DHCP server found in the System->Services menu, users may not be able to login the second time.

The enable dhcp client option allows you to turn on the dhcp client for this interface.

DHCP auto-auth configuration

The dhcp auto-auth configuration will allow you to configure automatic authentication and address assignment. Selecting auth-auth configuration (see fig 12) will bring up a configuration box (see fig 13).

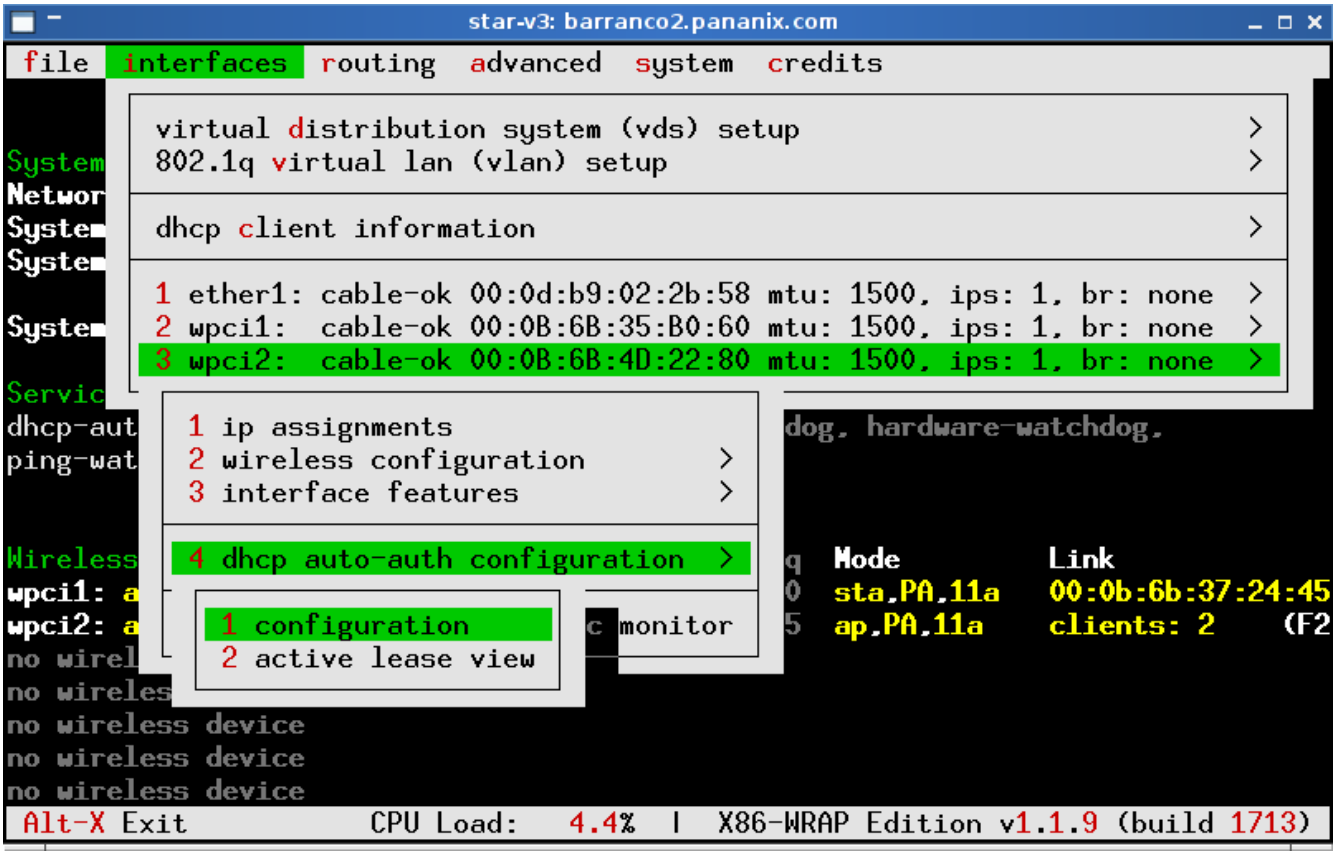


fig 12: dhcp auto-auth configuration

Basically, the information is the same as for any DHCP server, with the exception that you have two checkboxes: use radius, and create hotspot session. These permit a RADIUS server to perform authentication, and the session created by auto-auth be a “hotspot session”.

The Lease Duration is in seconds, the default of 1700 corresponding to 28 minutes. Other entries should be self-explanatory.

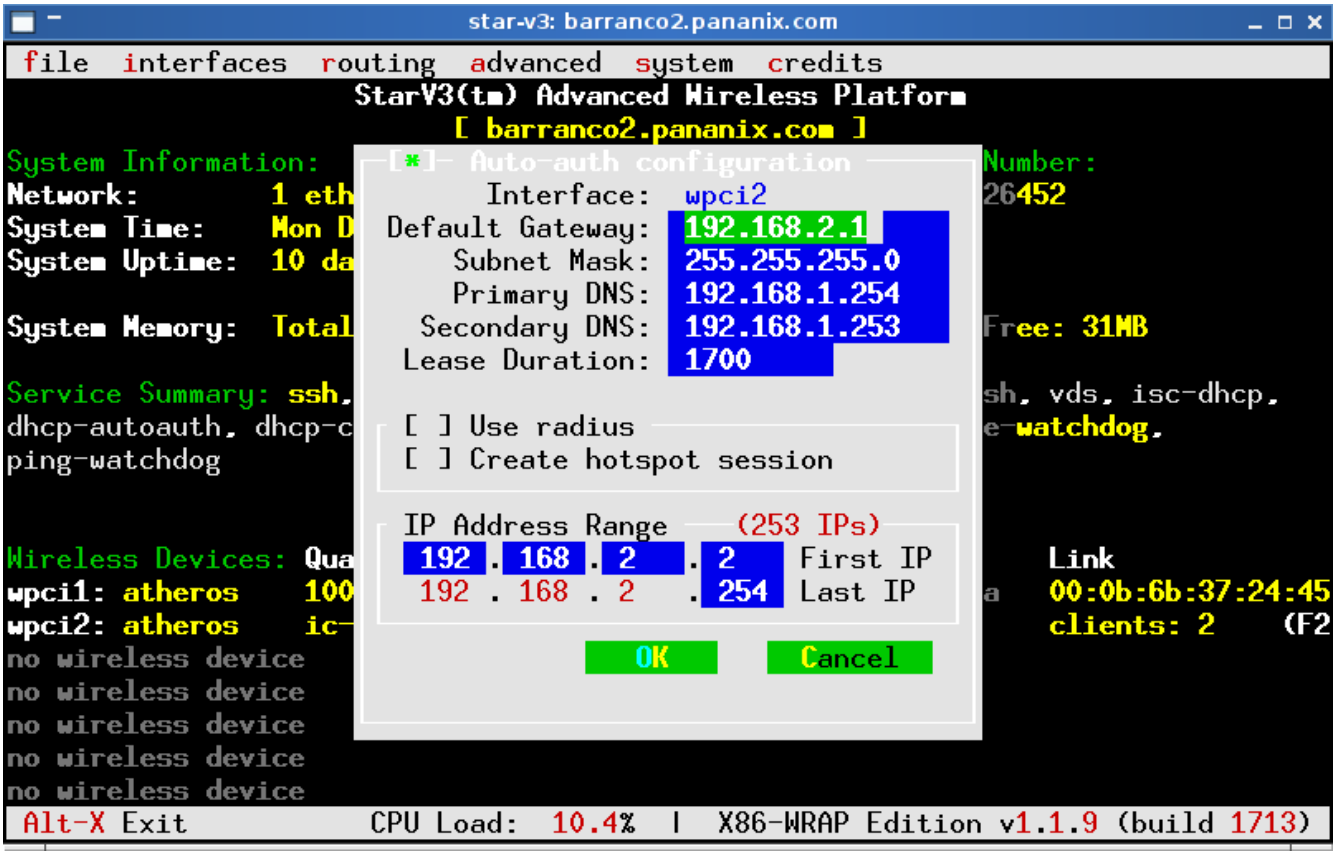


fig 13: auto-auth configuration menu

Beacon real-time traffic monitor

The beacon real-time traffic monitor (see fig 2) will allow you to see visually communications passing through the selected interface. Selecting this option presents the user with the box shown in fig 14.

First select those options you want to display. Always displayed is the rate or count. If no display options are selected before selecting Start, only one line will be displayed showing the selected rate or count. The filter options will allow you to specify any of protocol, source IP/mask or port,and destination IP/mask or port.

Changes to any of the display or filter options requires you to restart the monitor.

Sorting options allows you to choose between high-to-low or low-to-high. You may also choose one of the following seven options as well: source IP, destination IP, source port, destination port, receive, transmit (rate or count depending on display options), or protocol. Sorting options apply immediately with no need to restart the monitor.

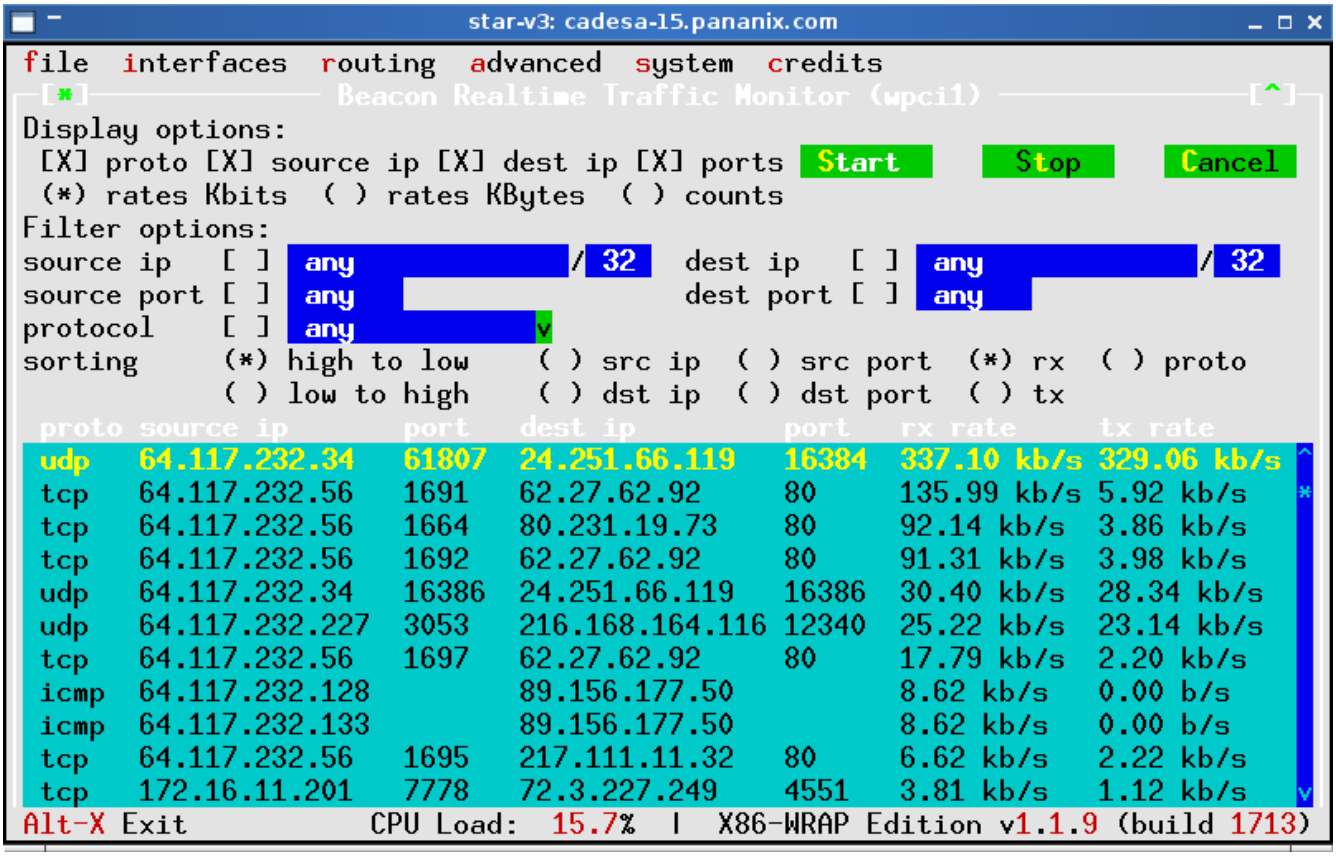

star-v3: cadesa-15.pananix.com
file interfaces routing advanced system credits
Beacon Realtime Traffic Monitor (wpci1)
Display options:
[X] proto [X] source ip [X] dest ip [X] ports
Start
Stop
Cancel
(*) rates Kbits ( ) rates KBytes ( ) counts
Filter options:
source ip [ ] any / 32 dest ip [ ] any / 32
source port [ ] any dest port [ ] any
protocol [ ] any
sorting (*) high to low ( ) src ip ( ) src port (*) rx ( ) proto
( ) low to high ( ) dst ip ( ) dst port ( ) tx
proto source ip port dest ip port rx rate tx rate
udp 64.117.232.34 61807 24.251.66.119 16384 337.10 kb/s 329.06 kb/s
tcp 64.117.232.56 1691 62.27.62.92 80 135.99 kb/s 5.92 kb/s
tcp 64.117.232.56 1664 80.231.19.73 80 92.14 kb/s 3.86 kb/s
tcp 64.117.232.56 1692 62.27.62.92 80 91.31 kb/s 3.98 kb/s
udp 64.117.232.34 16386 24.251.66.119 16386 30.40 kb/s 28.34 kb/s
udp 64.117.232.227 3053 216.168.164.116 12340 25.22 kb/s 23.14 kb/s
tcp 64.117.232.56 1697 62.27.62.92 80 17.79 kb/s 2.20 kb/s
icmp 64.117.232.128 89.156.177.50 8.62 kb/s 0.00 b/s
icmp 64.117.232.133 89.156.177.50 8.62 kb/s 0.00 b/s
tcp 64.117.232.56 1695 217.111.11.32 80 6.62 kb/s 2.22 kb/s
tcp 172.16.11.201 7778 72.3.227.249 4551 3.81 kb/s 1.12 kb/s
Alt-X Exit CPU Load: 15.7% | X86-WRAP Edition v1.1.9 (build 1713)

fig 14: beacon real-time traffic monitor

DHCP Client Information

If and only if this interface is a dhcp client, then you can access information regarding the active lease. or renew the lease information (see fig 15). This is grayed out when dhcp client is not active.

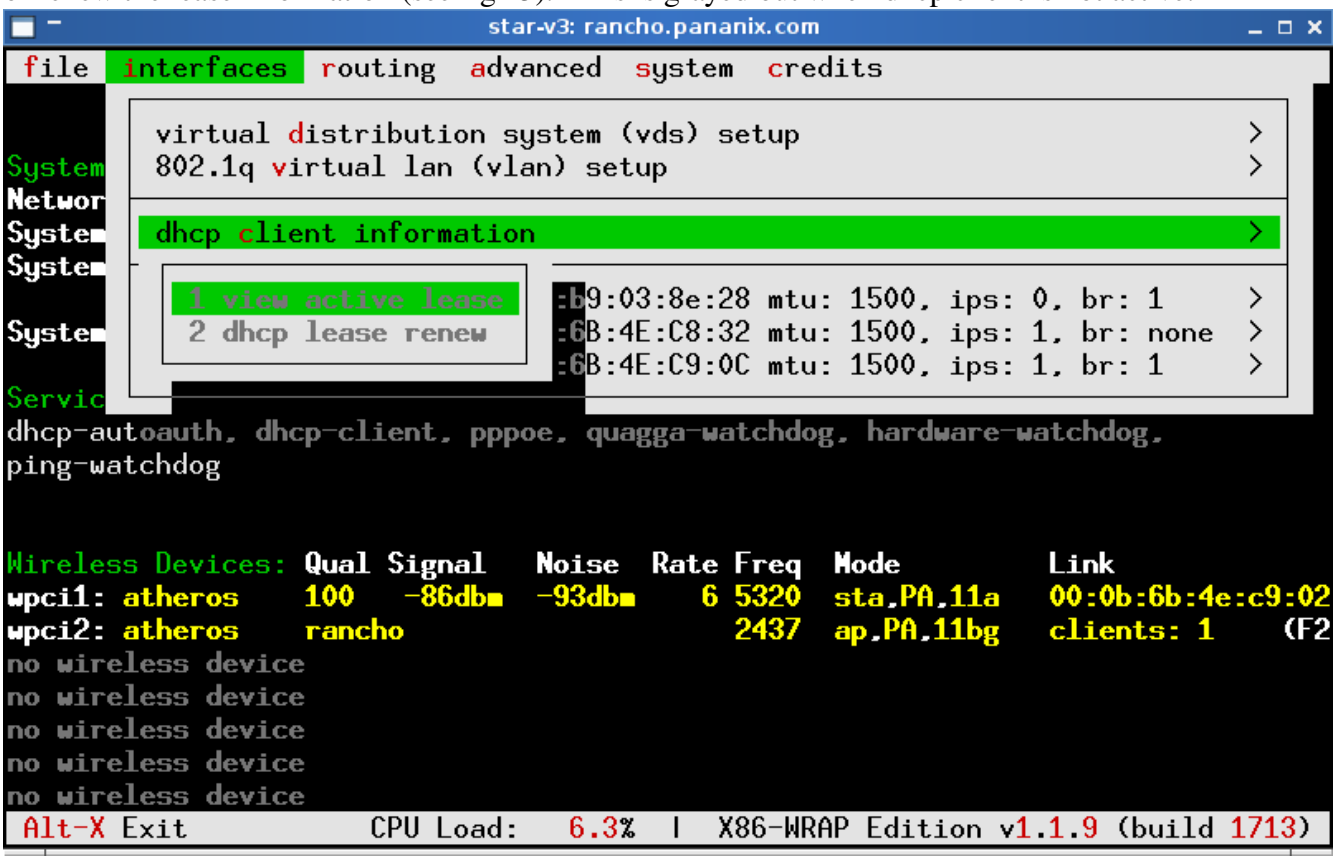

star-v3: rancho.pananix.com
file interfaces routing advanced system credits
virtual distribution system (vds) setup
802.1q virtual lan (vlan) setup
dhcp client information
1 view active lease
2 dhcp lease renew
dhcp-autoauth, dhcp-client, pppoe, quagga-watchdog, hardware-watchdog,
ping-watchdog
Wireless Devices: Qual Signal Noise Rate Freq Mode Link
wpci1: atheros 100 -86db -93db 6 5320 sta,PA,11a 00:0b:6b:4e:c9:02
wpci2: atheros rancho 2437 ap,PA,11bg clients: 1
no wireless device
no wireless device
no wireless device
no wireless device
no wireless device
Alt-X Exit CPU Load: 6.3% | X86-WRAP Edition v1.1.9 (build 1713)

fig 15: dhcp client information/renewal

802.1q Virtual Lan (VLAN) Setup

The VLAN setup is accessed from the interfaces menu (see fig 2). When selected, a setup box appears (see fig 16). VLAN's are frames that carry special tags in the headers. You can tag traffic with VLAN 0 to 4094, but if you have any Cisco gear, you should not use either 0 or 1.

The VLAN is attached to a physical device (ether1, ether2, wpci1, wpci2, etc.).

The reorder header checkbox should not be selected unless you have a problem with DHCP leases. Some DHCP servers require the headers reordered, but try without first.

You may also change the MAC address associated with VLAN traffic. This too, is often not a good idea unless you have a specific reason to do so.

The virtual device created then has a submenu similar to the physical devices. Here, you can change the MTU if you have problems passing larger packets, assign IP addresses, bridge them to other devices.

VLANs are used when you need to run two networks over the same wire or wireless link, but want to

keep the traffic separated.

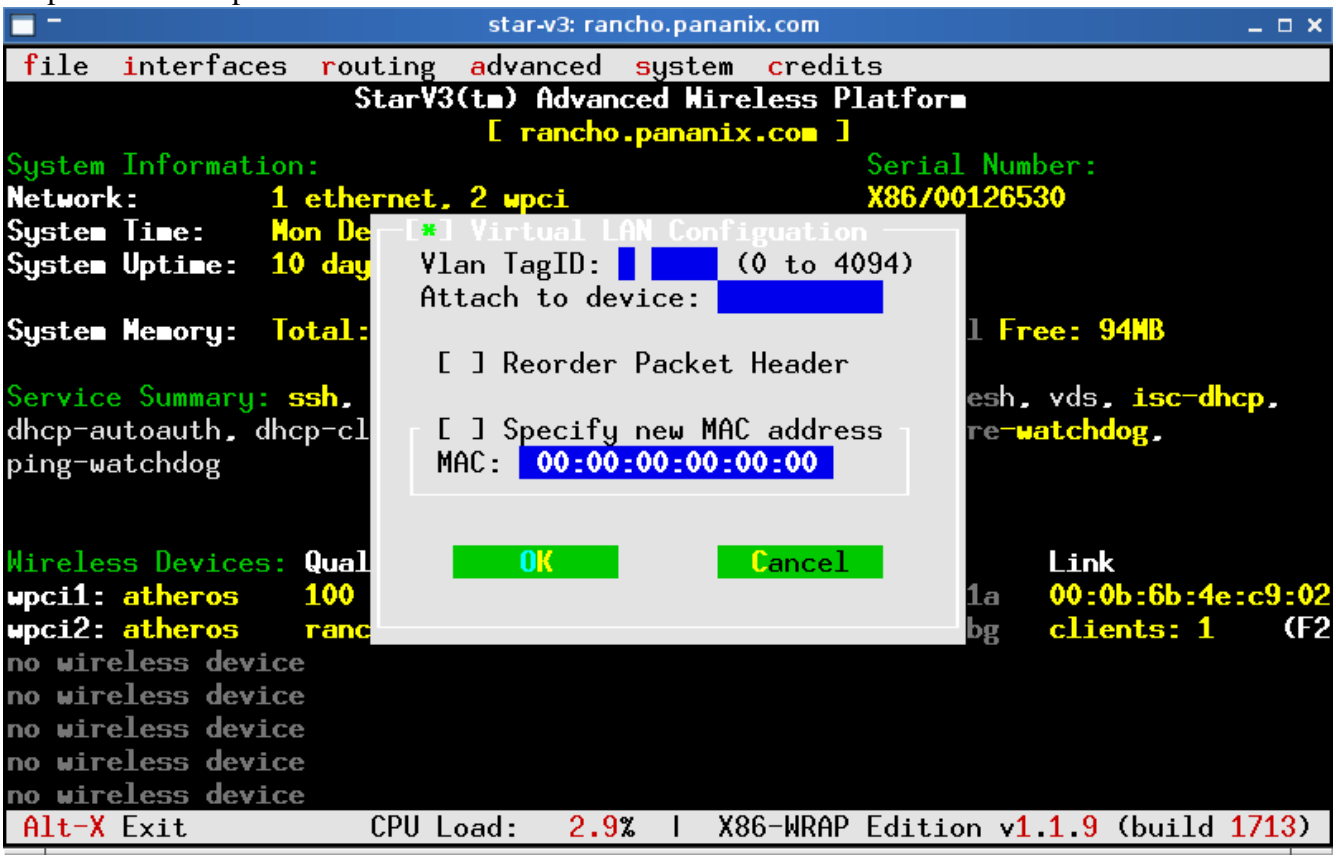


fig 16: VLAN configuration box

Virtual Distribution System (VDS) Setup

The Virtual Distribution System (VDS) is basically a VPN that permits the creation of a virtual circuit from one end to another. VDS will allow you to create an ethernet bridge between any two radios, but unlike most ethernet bridges you purchase, with VDS you can have several radios in between. See below for how to create an ethernet bridge between two radios.

First, select interfaces->virtual distribution system (vds) setup. Then select create new vds (see fig 17). This will provide you with a setup box (see fig 18).

Each VDS has only two endpoints, one server and one or more clients. The VDS can be a multipoint circuit. Select either server or client. You must put a username and password. This username and password will be used on each client that connects to a given server. Each side can have bandwidth limits. Each client should have its own bandwidth limits. Limits placed on the server will apply to all clients. So if you have 5 clients with 256KB limits and a server with 1MB limits, each client will get up to 256K, but that may be less if all clients are downloading at the same time, in which case they will each see a maximum of 200K due to the server limits of 1Mb total unless the CBQ method is per user.

The server side controls the circuit settings. Compression and encryption are optional, but take some small amount of CPU. If you have a requirement to maintain a data stream confidential over a wireless circuit, this is one way to ensure confidentiality. The VDS uses AES encryption. Select Multipoint if the server will have multiple clients. Multipoint VDS' may only be bridges, so must be bridged with another interface.

Clients must be told where to find the server (IP). Servers should not enter anything here.

Creating an Ethernet Bridge

To create an ethernet bridge, first set up two radios. Do not create any bridges at this point. The two wireless cards connected to each other should be on one network (e.g., 192.168.20.13/30 and 192.168.20.14/30). The ethernet interfaces should have IPs on the network to be bridged (e.g., 10.10.1.100/24 and 10.10.1.102/24). Create a VDS and bridge each VDS to the ethernet devices. Your vds client (192.168.20.14) should point at the wireless device on the server (192.168.20.13). It's that easy.

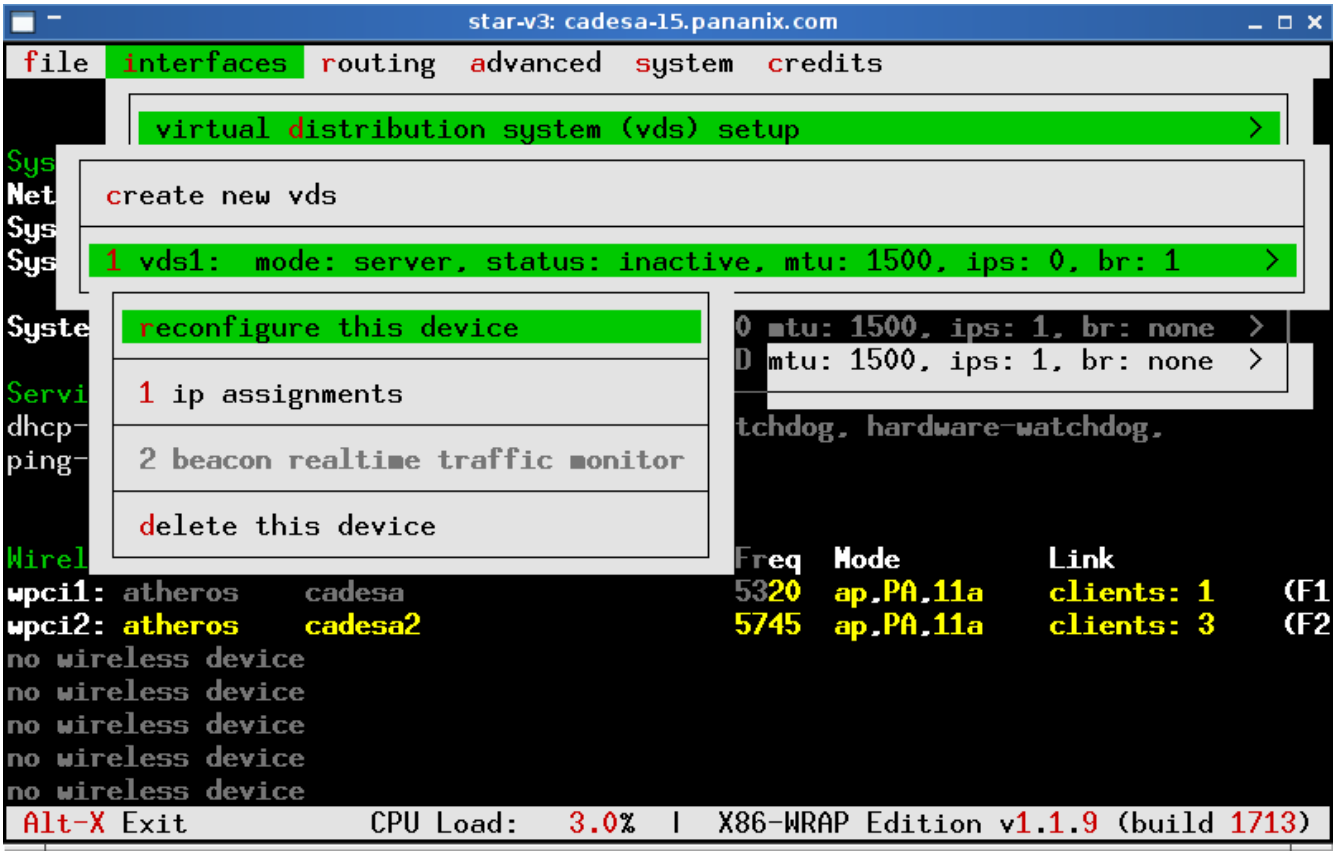

star-v3: cadesa-15.pananix.com
file interfaces routing advanced system credits
virtual distribution system (vds) setup
create new vds
1 vds1: mode: server, status: inactive, mtu: 1500, ips: 0, br: 1
reconfigure this device
1 ip assignments
2 beacon realtime traffic monitor
delete this device
mtu: 1500, ips: 1, br: none
mtu: 1500, ips: 1, br: none
tchdog, hardware-watchdog,
Freq Mode Link
wpci1: atheros cadesa 5320 ap,PA,11a clients: 1 (F1
wpci2: atheros cadesa2 5745 ap,PA,11a clients: 3 (F2
no wireless device
no wireless device
no wireless device
no wireless device
no wireless device
Alt-X Exit CPU Load: 3.0% | X86-WRAP Edition v1.1.9 (build 1713)

fig 17: vds submenu

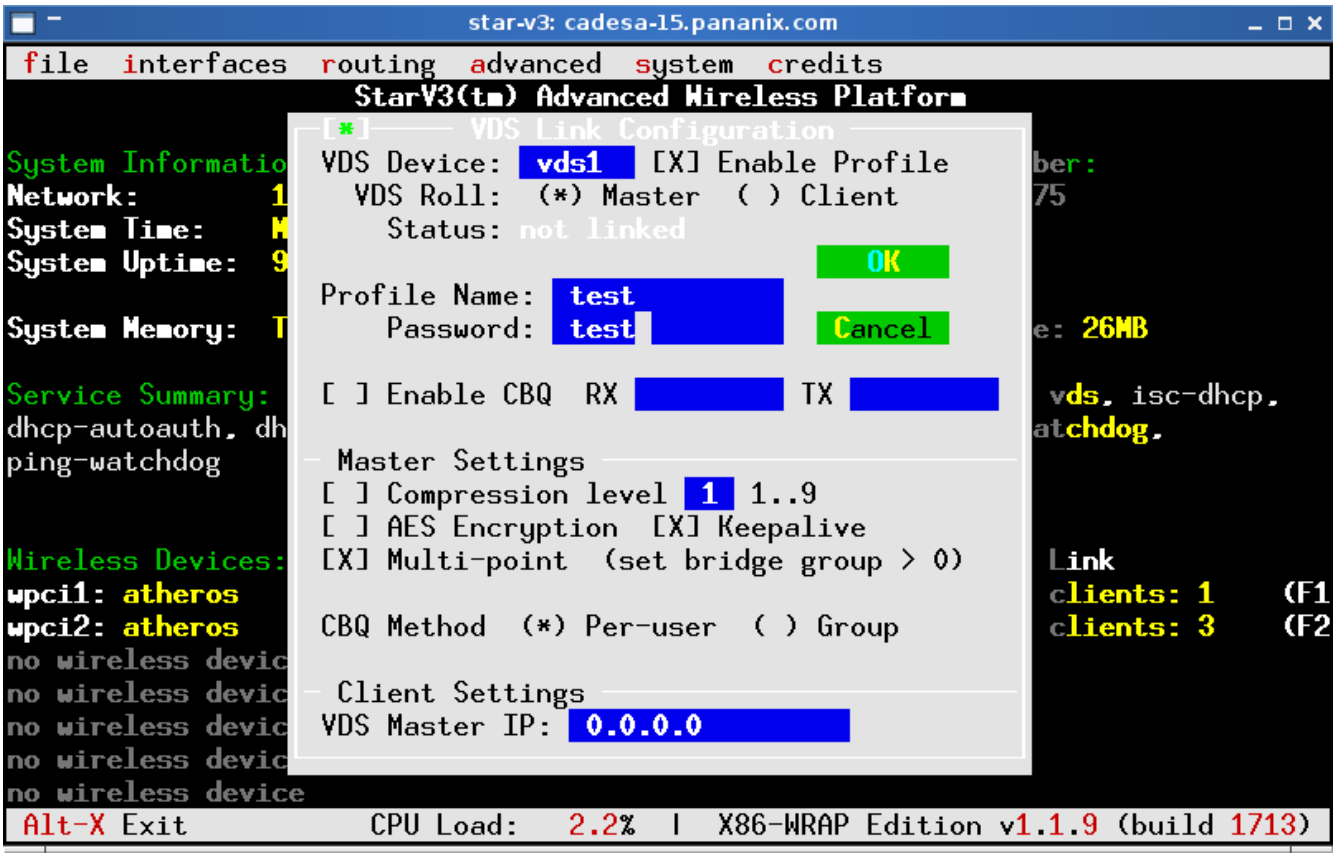


fig 18: vds setup box

Chapter 5

Routing Menu

While a very short menu, it is an important one. It would be difficult to do much of anything without routing.

Configuring routing

The routing menu is split into two parts (see fig 1). The upper part is basic routing and routing daemons. The lower part is advanced and policy routing. Since it is unlikely you'll have a system without at least a default route, we'll start there. The rest will follow.

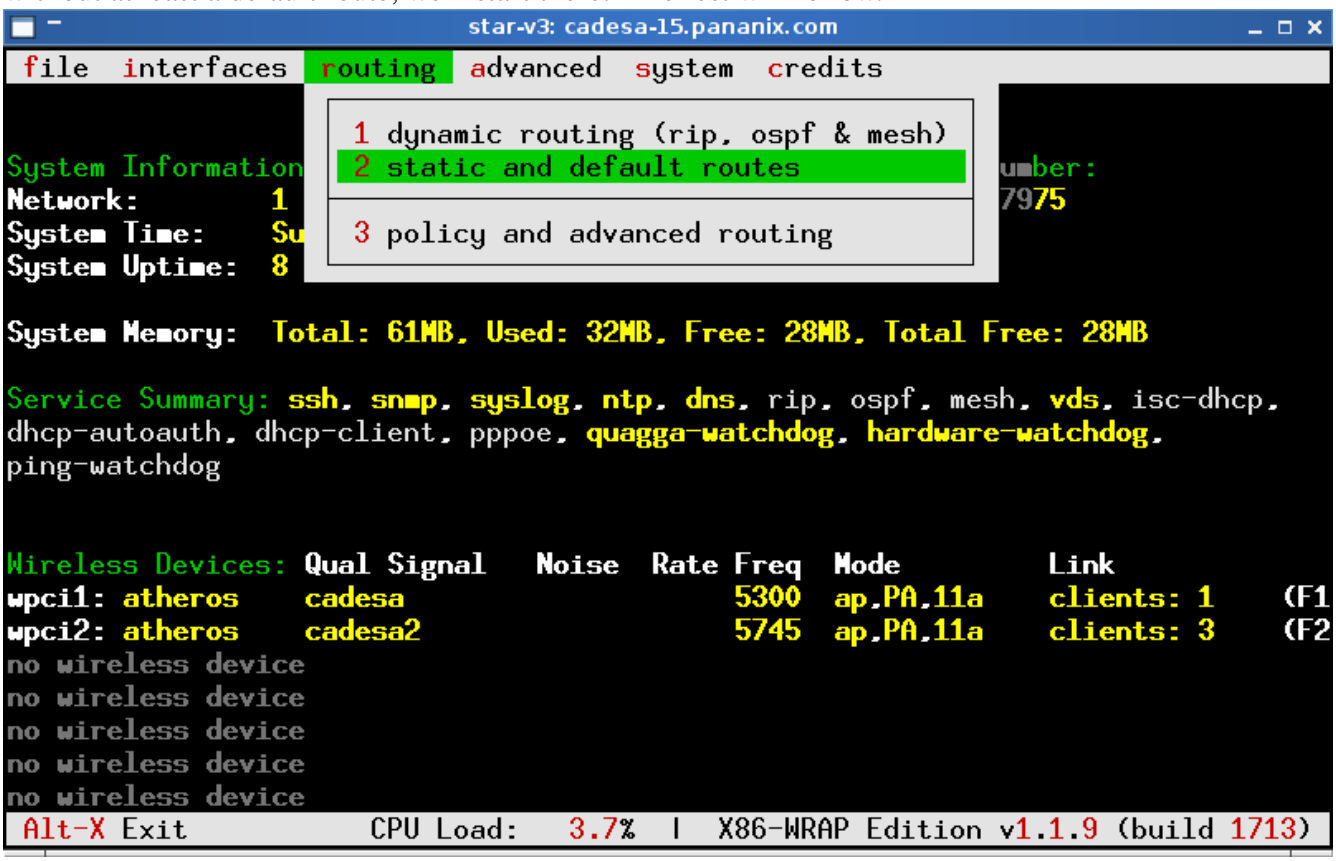

star-v3: cadesa-15.pananix.com
file interfaces routing advanced system credits
1 dynamic routing (rip, ospf & mesh)
2 static and default routes
3 policy and advanced routing
System Information
Network: 1
System Time: Su
System Uptime: 8
umber:
7975
System Memory: Total: 61MB, Used: 32MB, Free: 28MB, Total Free: 28MB
Service Summary: ssh, snmp, syslog, ntp, dns, rip, ospf, mesh, vds, isc-dhcp, dhcp-autoauth, dhcp-client, pppoe, quagga-watchdog, hardware-watchdog, ping-watchdog
Wireless Devices: Qual Signal Noise Rate Freq Mode Link
wpci1: atheros cadesa 5300 ap,PA,11a clients: 1 (F1
wpci2: atheros cadesa2 5745 ap,PA,11a clients: 3 (F2
no wireless device
no wireless device
no wireless device
no wireless device
no wireless device
Alt-X Exit CPU Load: 3.7% | X86-WRAP Edition v1.1.9 (build 1713)

fig 1: the routing menu

Static and default routes

The static and default routes can be set by selecting the static and default routes menu item (see fig 1). A configuration box will present itself (see fig 2).

The default route is the first line, shown by 0.0.0.0/0 and the IP of the gateway to the world.

All routes must point to an IP on a network on the radio. If not, you'll see a '!' following the line number. Effectively, this means the route is disabled. It does not mean the IP pointed to is unreachable.

If you disable a route, the route will have a '*' following the line number, as in fig 2 below.

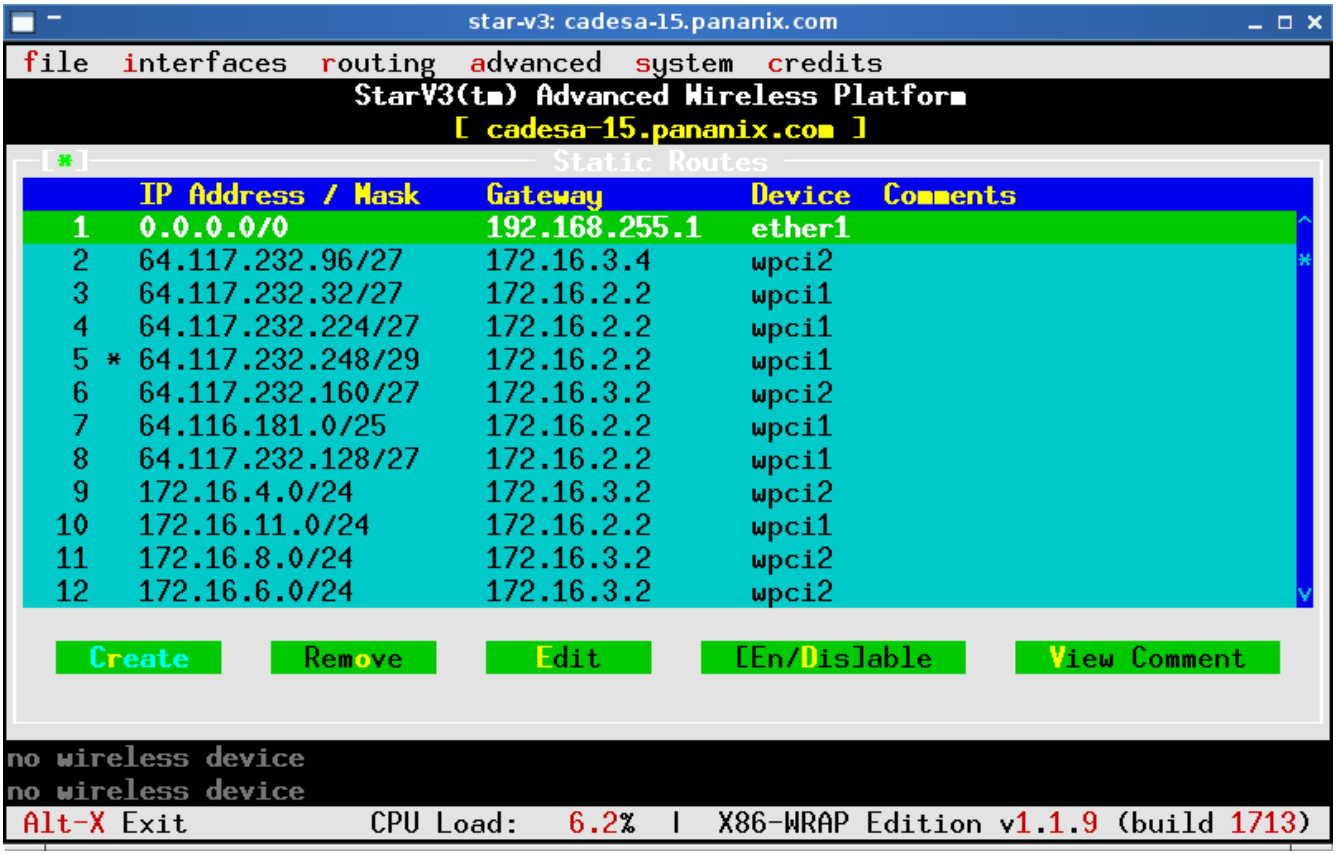


fig 2: Static routes configuration box

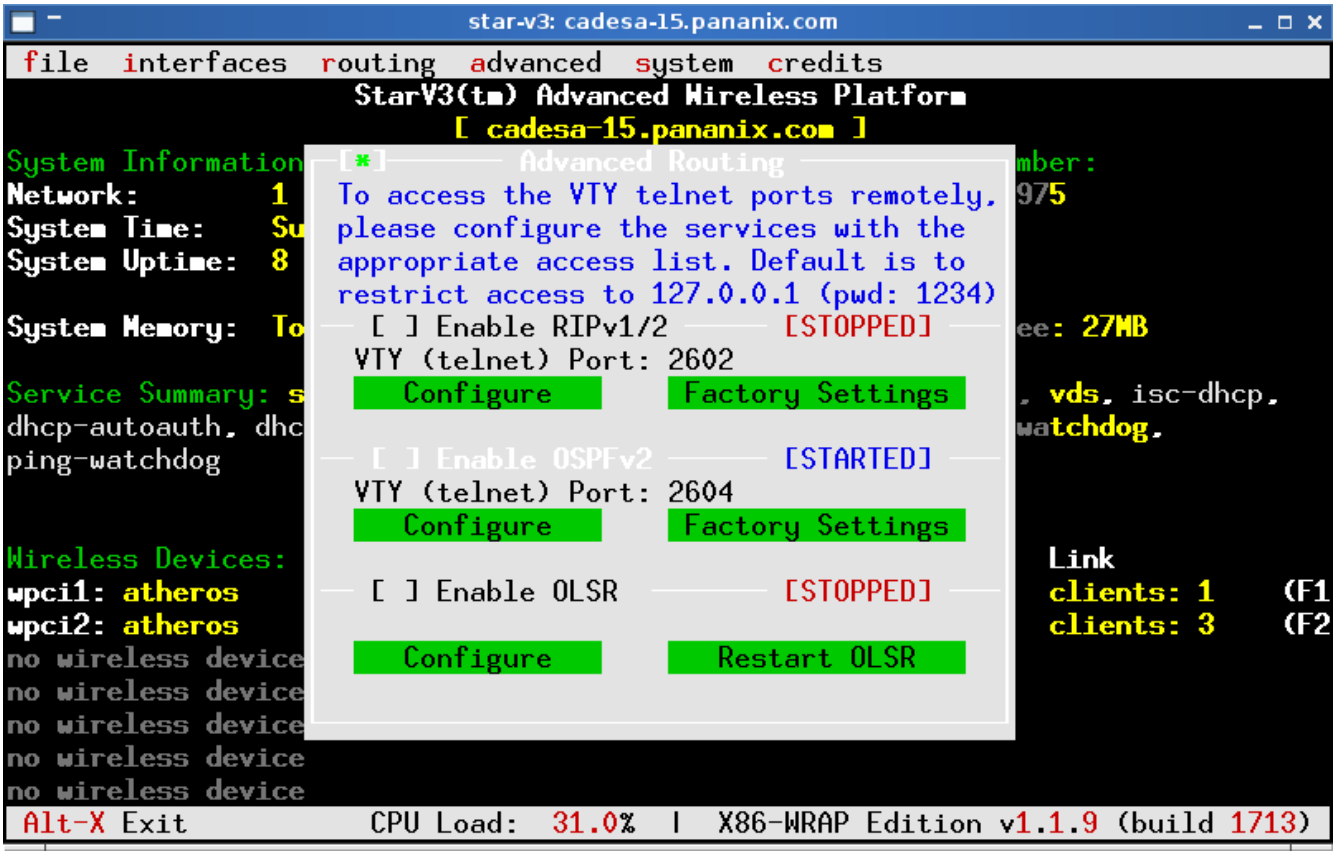
Dynamic Routing

Selecting dynamic routing (rip, ospf & mesh) provides you with an option to use one of the dynamic routing methods available in StarOS. The three selections you have are as follows:

- RIPv1/2: activates and provides configuration access to only RIP
- OSPFv2: activates and provides configuration access to OSPF, BGP, and RIP
- OLSR: activates and provides configuration access to mesh routing

Selecting any one will activate that service (see fig 3). The static routes in fig 2 above are a prime candidate for dynamic routing via OSPF.

Enabling OSPF in one radio is like only having one radio, though. With no neighbor(s) to talk to, the OSPF daemon has no peers to share routing information with. So the same service must be started on those systems connected to this one.


star-v3: cadesa-15.pananix.com
file interfaces routing advanced system credits
StarV3(tm) Advanced Wireless Platform
[cadesa-15.pananix.com]
Advanced Routing
To access the VTY telnet ports remotely, please configure the services with the appropriate access list. Default is to restrict access to 127.0.0.1 (pwd: 1234)
[ ] Enable RIPv1/2 [STOPPED]
VTY (telnet) Port: 2602
Configure Factory Settings
[ ] Enable OSPFv2 [STARTED]
VTY (telnet) Port: 2604
Configure Factory Settings
[ ] Enable OLSR [STOPPED]
Configure Restart OLSR
Alt-X Exit CPU Load: 31.0% | X86-WRAP Edition v1.1.9 (build 1713)
fig 3: dynamic routing daemons startup/shutdown screen

Once started, you can access the configuration menu (see fig 4) by selecting “Configure”. In the case of OSPF, you should at least configure the default route.

For those of you familiar with Cisco console menus, the routing daemon console menus function in the same way (see fig 4). When in doubt, entering a question mark '?' will provide a context sensitive list of available options. Also for those familiar with Cisco, the same shortcuts exist, e.g., using 'en' for enable.

The RIP daemon console is similar to the OSPF console.

The OLSR configuration screen is more like the standard StarOS configuration screens (see fig 5). OLSR is preconfigured to a working configuration that should fit a large majority of users. Advanced users may want to tweak these settings.

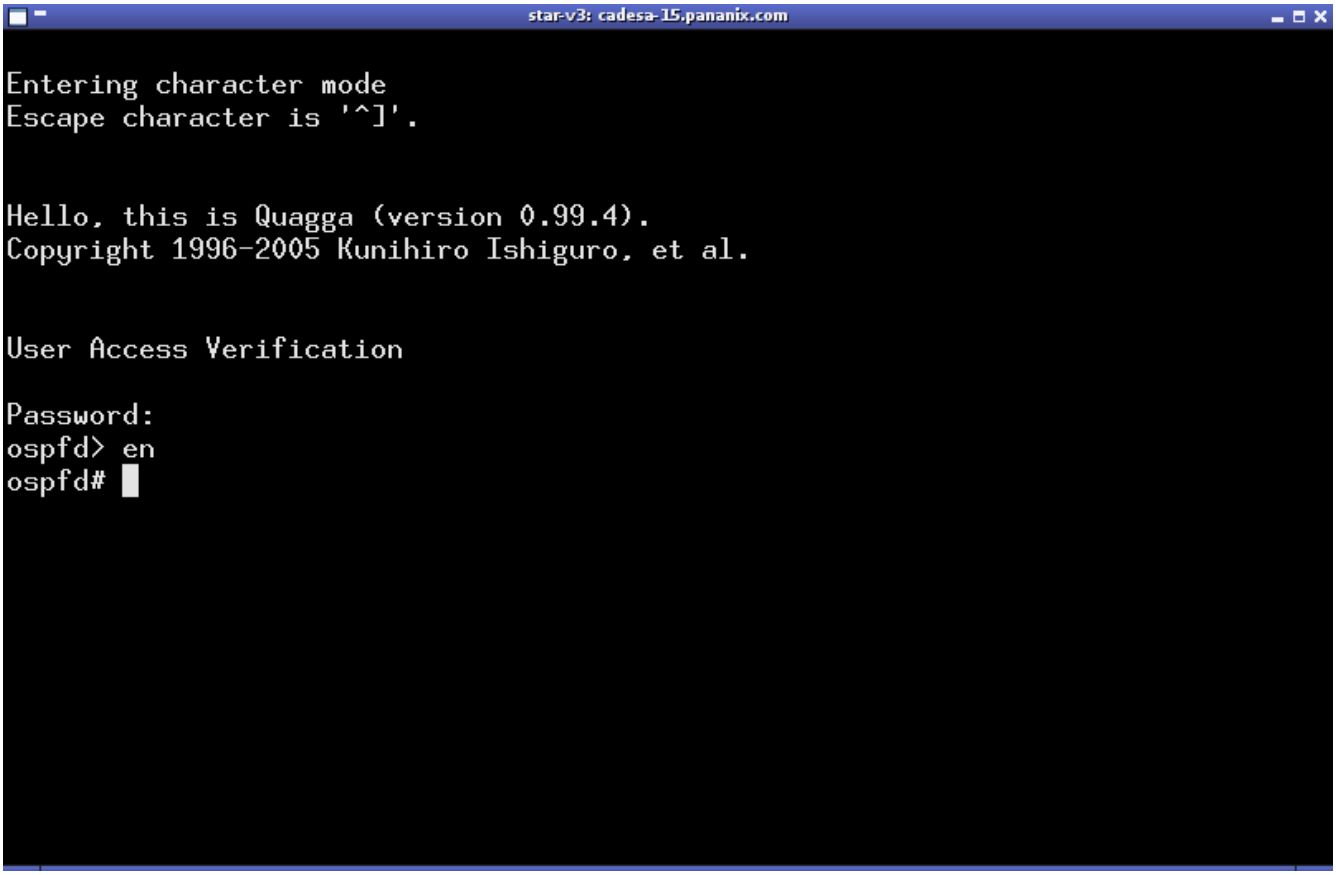


fig 4: daemon configuration console

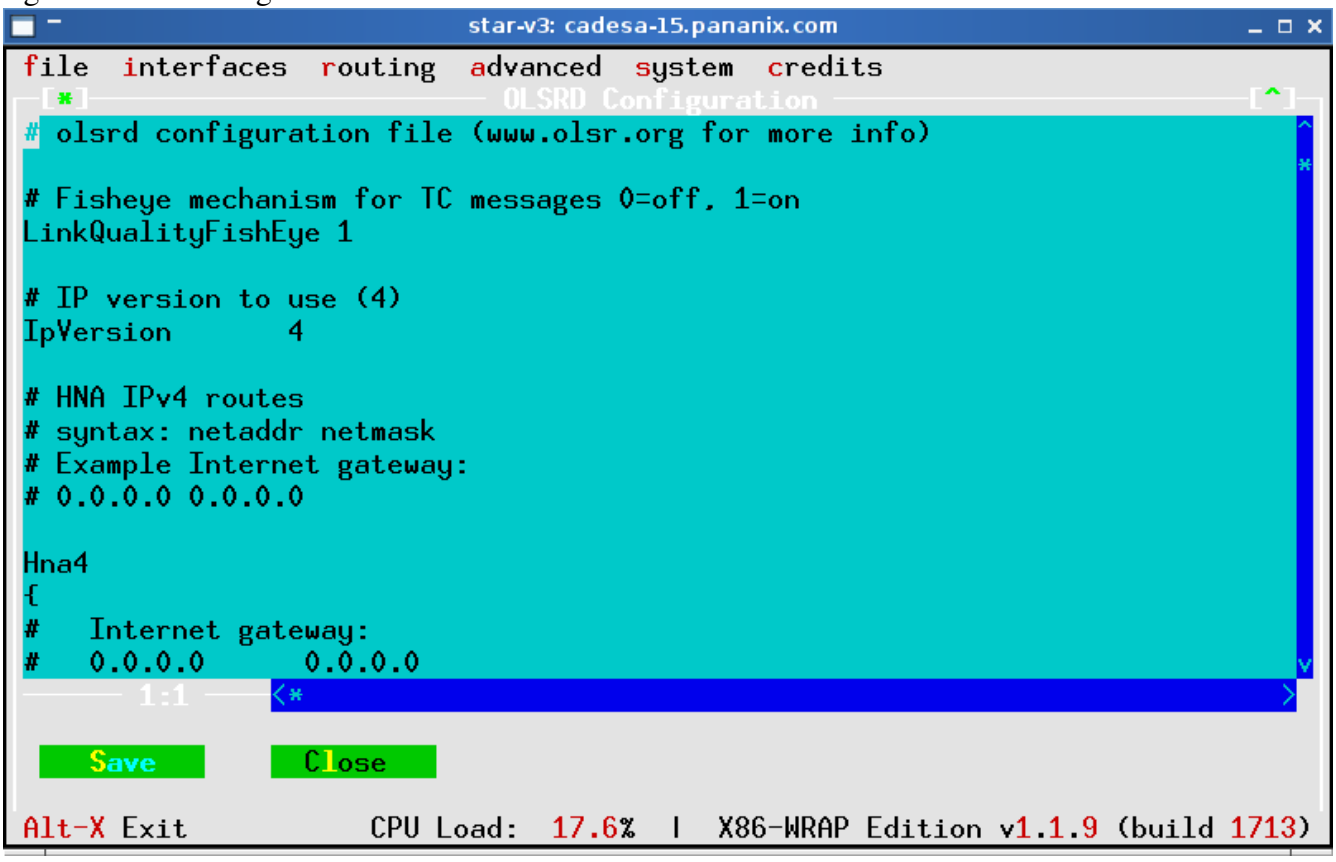


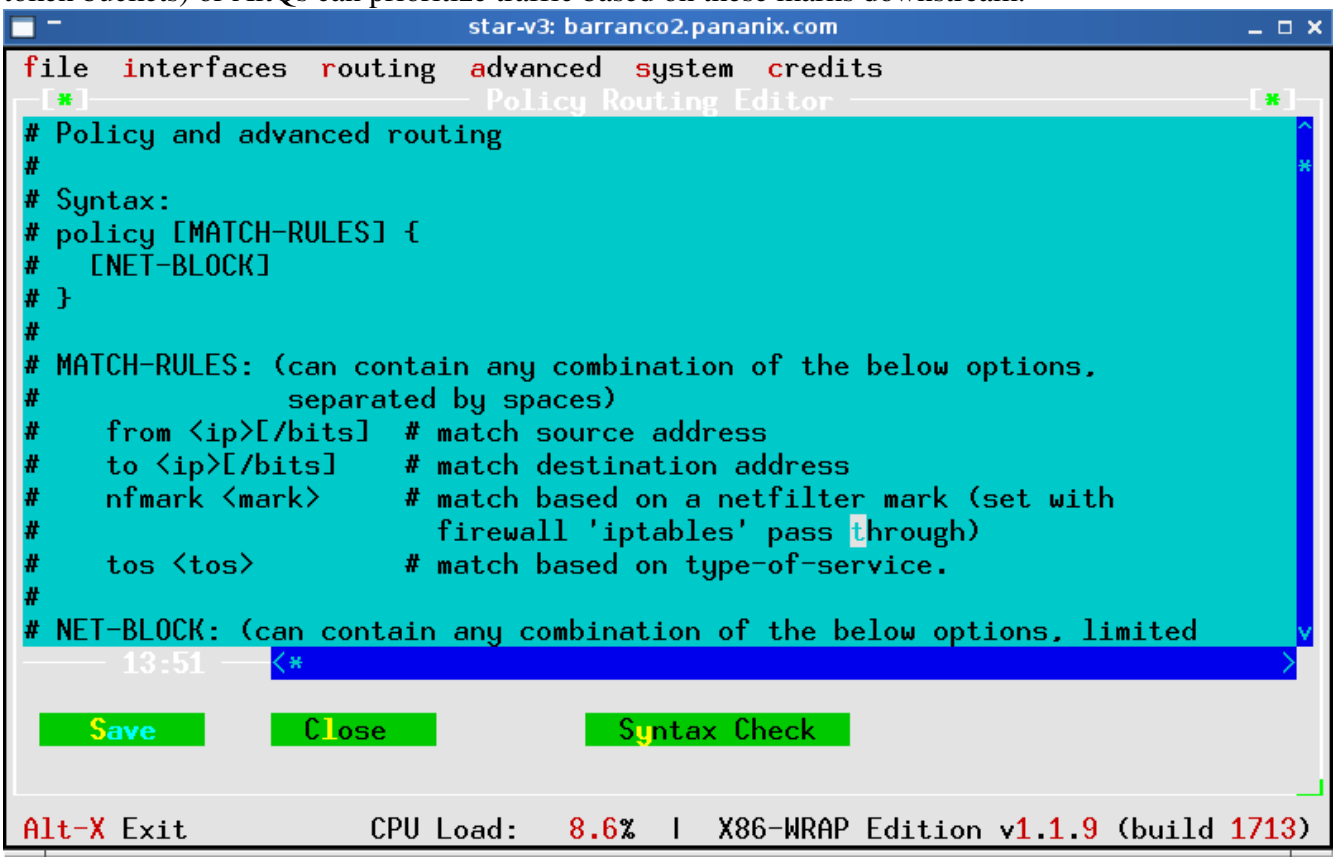
fig 5: olsr configuration console

Policy and Advanced Routing

The policy and advanced routing section allows you to do some funky routing tricks (see fig 6).

Policy routing allows you to route different networks out different gateways, such as if you have two downstream providers. You can route each ones packets out correctly.

Advanced routing works similarly, but uses firewall marks (see Advanced menu chapter) to route packets. For example, if you want to reserve one low-latency link solely for SIP VoIP traffic while routing P2P traffic out a slow link. Routers using prioritizing traffic shapers such as HTB (heirarchical token buckets) or AltQs can prioritize traffic based on these marks downstream.


star-v3: barranco2.pananix.com
file interfaces routing advanced system credits
Policy Routing Editor
Policy and advanced routing
#
Syntax:
policy [MATCH-RULES] {
[NET-BLOCK]
}
#
MATCH-RULES: (can contain any combination of the below options,
separated by spaces)
from <ip>[/bits] # match source address
to <ip>[/bits]   # match destination address
nfmark <mark>   # match based on a netfilter mark (set with
firewall 'iptables' pass through)
tos <tos>   # match based on type-of-service.
#
NET-BLOCK: (can contain any combination of the below options, limited
13:51
Save
Close
Syntax Check
Alt-X Exit
CPU Load: 8.6% | X86-WRAP Edition v1.1.9 (build 1713)
fig 6: policy and advanced routing configuration screen

Chapter 6

Advanced Menu

Without doubt, this menu will be the most used of all, particularly the last three items. Don't let the "Advanced" label scare you. A number of these items are extremely important to troubleshooting.

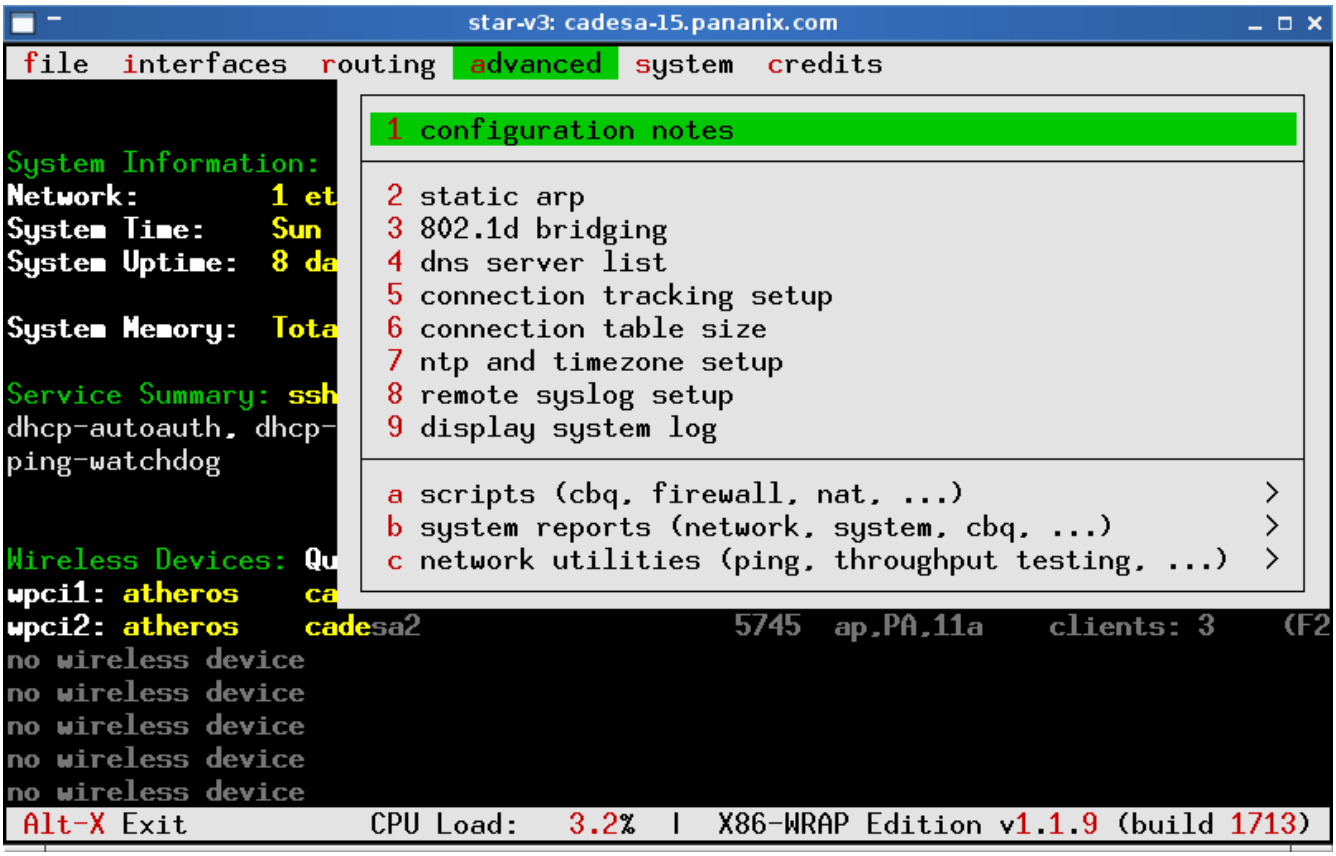

star-v3: cadesa-15.pananix.com
file interfaces routing advanced system credits
1 configuration notes
2 static arp
3 802.1d bridging
4 dns server list
5 connection tracking setup
6 connection table size
7 ntp and timezone setup
8 remote syslog setup
9 display system log
a scripts (cbq, firewall, nat, ...) >
b system reports (network, system, cbq, ...) >
c network utilities (ping, throughput testing, ...) >
System Information:
Network: 1 et
System Time: Sun
System Uptime: 8 da
System Memory: Tota
Service Summary: ssh
dhcp-autoauth, dhcp-
ping-watchdog
Wireless Devices: Qu
wpci1: atheros ca
wpci2: atheros cadesa2 5745 ap,PA,11a clients: 3 (F2
no wireless device
no wireless device
no wireless device
no wireless device
no wireless device
Alt-X Exit CPU Load: 3.2% | X86-WRAP Edition v1.1.9 (build 1713)

fig 1: the Advanced menu dropdown

Configuration notes

Here, you can record anything you want in narrative form about this radio. Completely optional, but a good idea for those who may need to look at this radio after you've been promoted.

Static ARP

Static ARP allows you to remap the arp table for directly connected hosts. Instructions are simple. Be careful with this, or you may be wondering why some hosts cannot be contacted. This should only be necessary for clients you haven't been able to reconfigure for your network and who have an IP hard-coded.

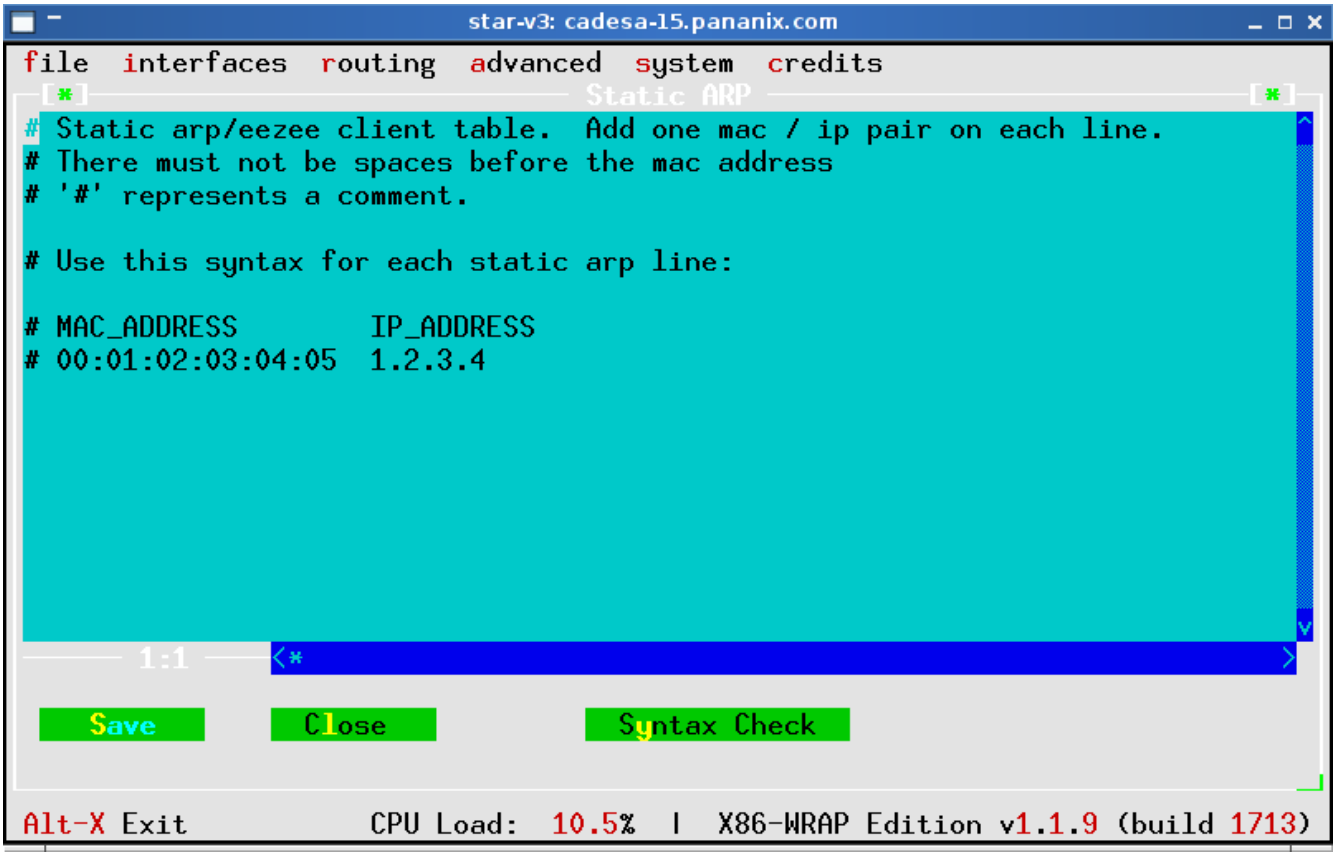

star-v3: cadesa-15.pananix.com
file interfaces routing advanced system credits
Static ARP
Static arp/eezee client table. Add one mac / ip pair on each line.
There must not be spaces before the mac address
'#' represents a comment.
Use this syntax for each static arp line:
MAC_ADDRESS IP_ADDRESS
00:01:02:03:04:05 1.2.3.4
1:1
Save
Close
Syntax Check
Alt-X Exit
CPU Load: 10.5% | X86-WRAP Edition v1.1.9 (build 1713)

fig 2: Static ARP menu

802.1d Bridging Options

Spanning tree protocol is used to prevent bridge loops. Unlike router loops, bridge loops could theoretically never time out because unlike routers, bridges do not decrement the TTL counter. If you have anything more than a simple ethernet bridge, you should leave STP enabled. The defaults suffice for most. The benefits of using STP far outweigh the detrimental effects of turning it off when it's needed.

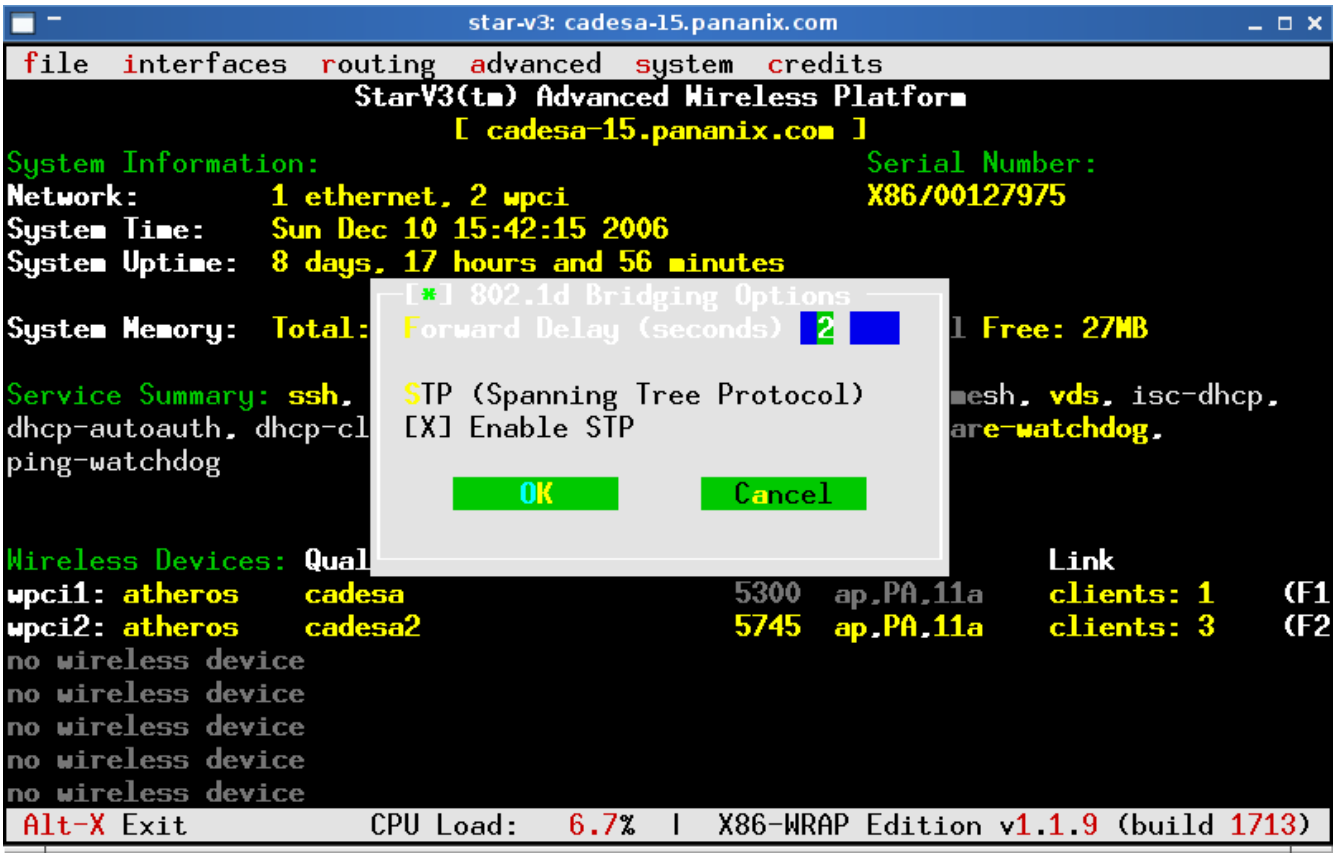


fig 3: 802.1d Bridging Options Menu

DNS Server List

The DNS server list configuration menu allows you to assign a name to your system and tell it which DNS servers to use. While in many instances you might think this unnecessary, you'll find that services like the dropbear SSH server respond more quickly with it. It also allows you to check connectivity using the ping and traceroute utilites with names vice IP only, and the ability to resolve names with tcpdump.

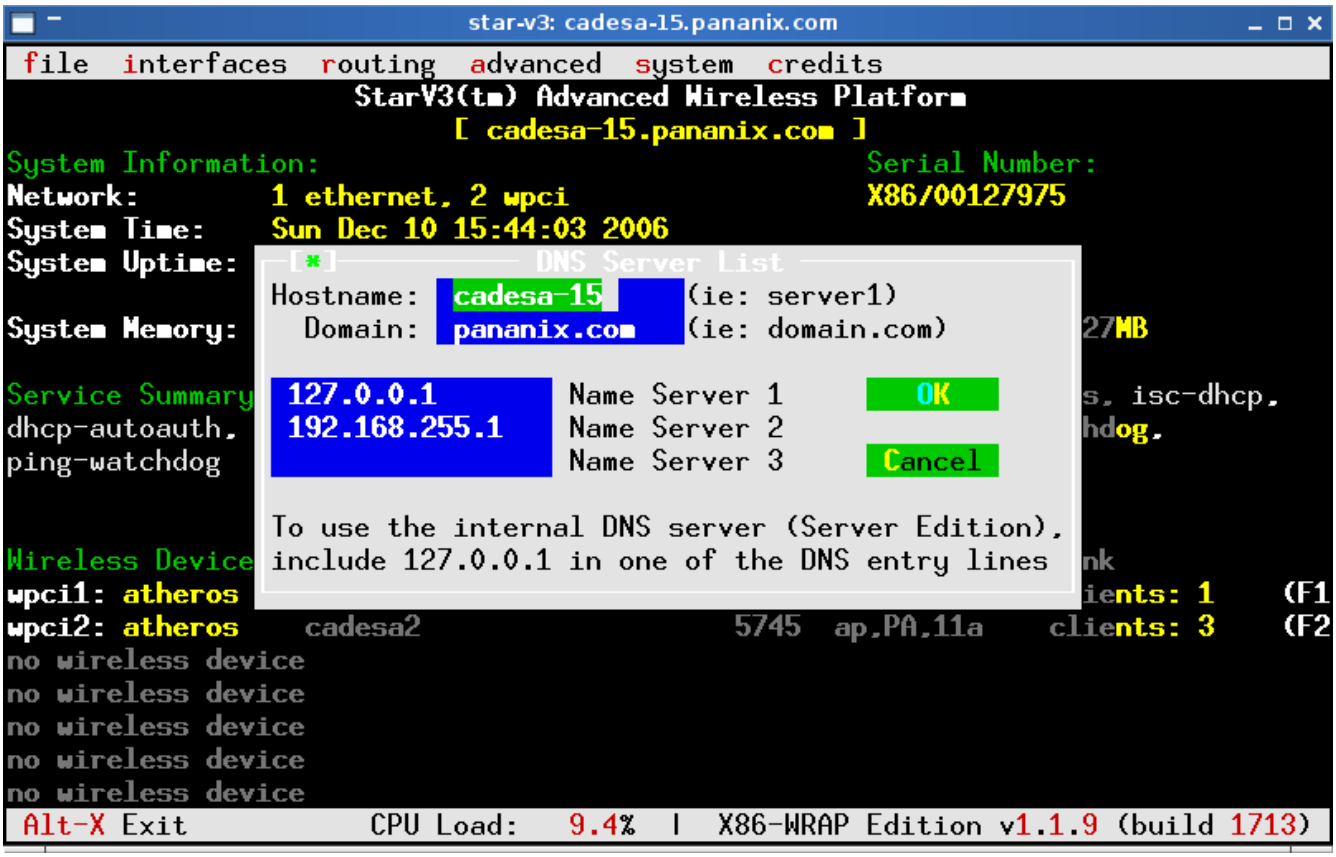


fig 4: DNS Server List menu

Connection Tracking Setup

Connection tracking setup is required for NAT. If you use NAT, you'll need to enable this, and you'll want to review which protocol helpers are enabled. If you don't enable the protocol helpers for these particular protocols, you'll find those protocols won't work properly for NATed clients.

The FTP helper is for active FTP sessions. Passive FTP session (such as those set up by most web browsers) will work just fine.

The IRC helper is for Internet Relay Chat.

The H323 helper is for those phones and programs (like Netmeeting) that use H323. Phones that use the SIP or IAX protocols are unaffected by this setting

The GRE (Generic Routing Encapsulation) protocol helper is used if you use GRE. Those working in Cisco environments may need to enable this.

The PPTP NAT helper enables point-to-point tunneling protocol help.

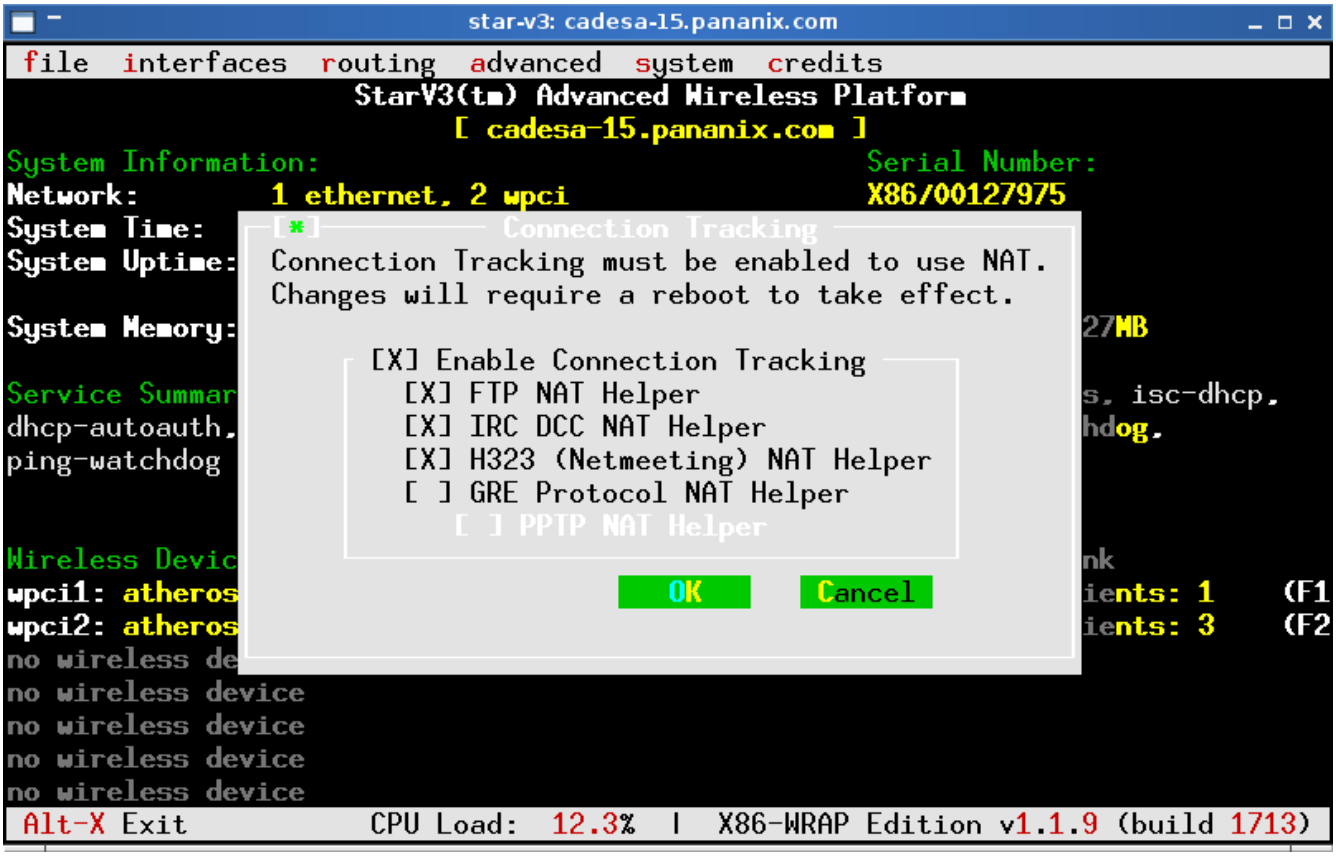


fig 5: Connection tracking table setup

Connection Table Size

The connection tracking table size configuration menu is used if you need to increase the size of your connection tracking table (used for NAT). Since each connection must be tracked to be properly routed back to clients, this table must be large enough to accommodate all simultaneous connections. Old connections are dropped after a period of time.

While sufficient table entries are required, particularly since most connections create several table entries, you want to ensure you don't try to create a table so large it uses all available memory. In fig 6 below, it would be imprudent to create a table taking more than about 15MB of memory (approx 48,000 rows). The default of 16384 rows should be sufficient for a large number of clients (depending on your traffic mix).

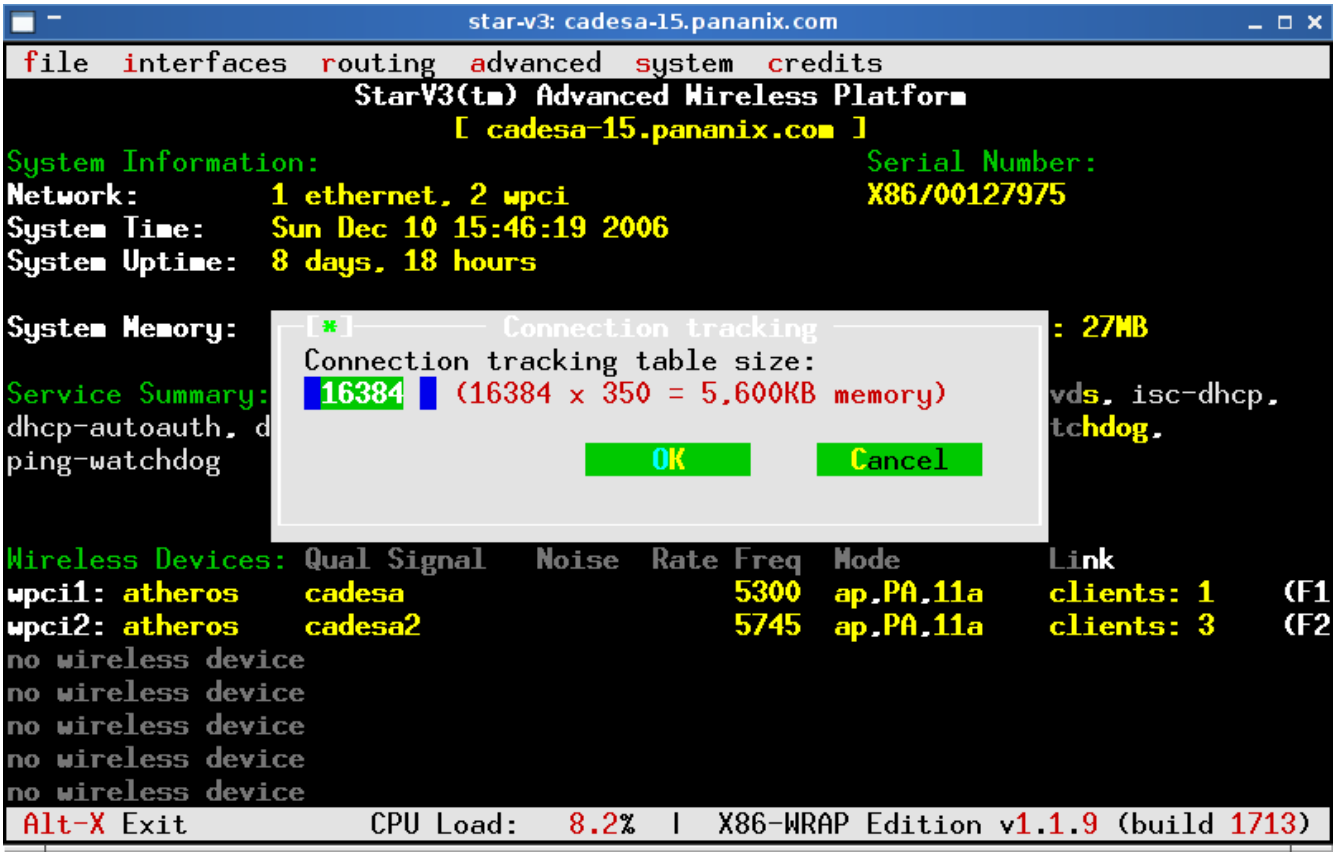


fig 6: Connection tracking table size menu

NTP and Zone configuration

If you configure nothing else, consider configuring your NTP server. Keeping your radios in time sync helps track problems in the logs, since they use the time according to the radio.

If you've configured your DNS servers (above) and don't have ntp, openntp, chrony, or other ntp daemons running on a system local to your network, you can always use the publicly available pool.ntp.org servers. Each time ntp starts, it will query pool.ntp.org and use one of the available ntp servers.

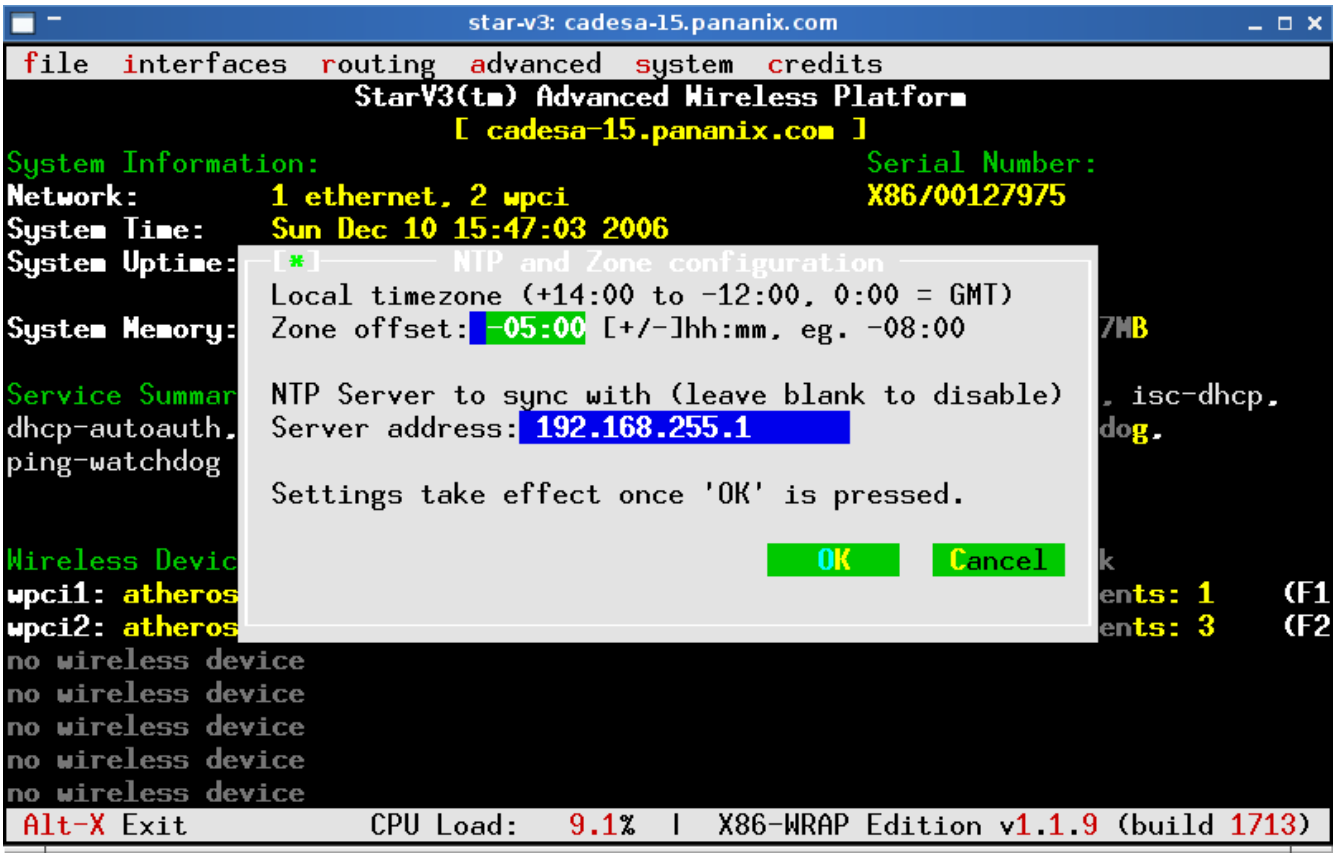


fig 7: NTP and Time Zone configuration menu

Remote Syslog

Using a remote syslog is highly recommended for troubleshooting because StarOS does not save syslog entries between reboots. To prepare for doing this, you'll need to set up a central logging server that starts the syslog daemon with the -r option. This will open UDP port 514 and accept syslog input from external hosts. To prevent DOS attacks, use a packet filter (pf in *BSD or iptables in Linux) to block unauthorized hosts.

Ensure you have set up NTP (above) so that you have accurate time records.

You may also need to reconfigure /etc/syslog.conf in your logging server to save the radio logs to the log file of your choice.

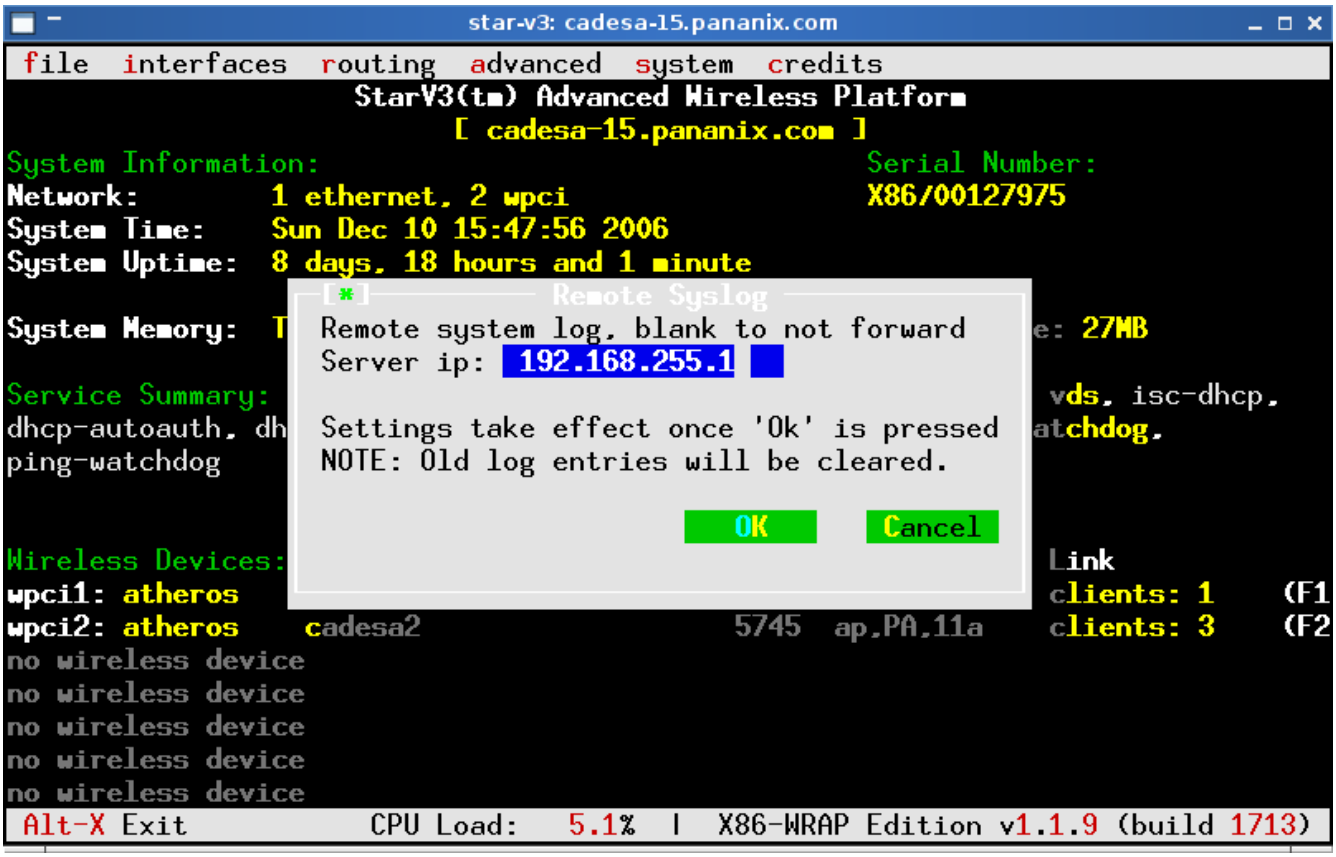


fig 8: Remote Syslog configuration menu

System Log

The system log can be reviewed via the system log box. This log is not saved between reboots or syslog restarts (such as when remote logging is configured, above). So for troubleshooting purposes, using remote logging is a good idea. You can still review the logs here even when using remote logging.

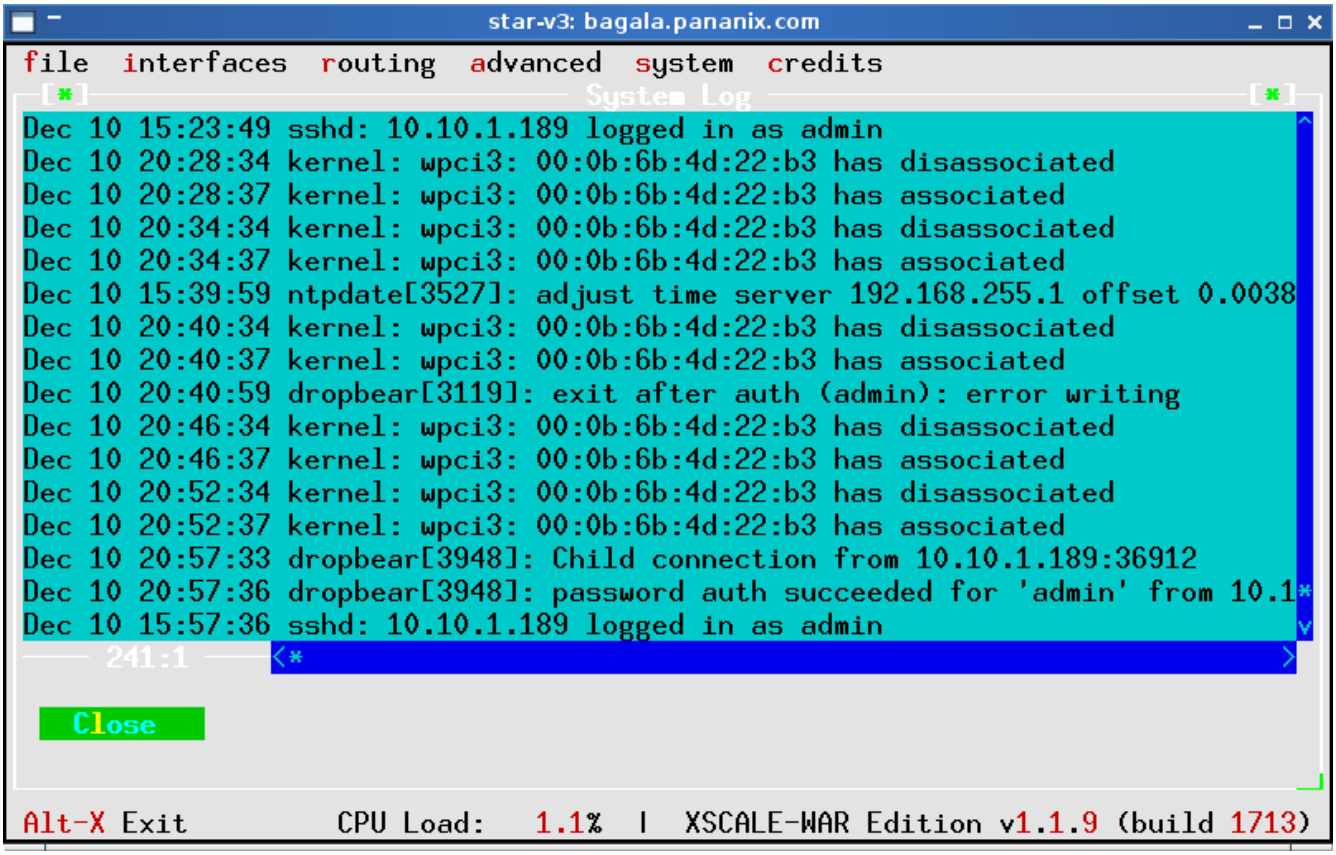

star-v3: bagala.pananix.com
file interfaces routing advanced system credits
System Log
Dec 10 15:23:49 sshd: 10.10.1.189 logged in as admin
Dec 10 20:28:34 kernel: wpci3: 00:0b:6b:4d:22:b3 has disassociated
Dec 10 20:28:37 kernel: wpci3: 00:0b:6b:4d:22:b3 has associated
Dec 10 20:34:34 kernel: wpci3: 00:0b:6b:4d:22:b3 has disassociated
Dec 10 20:34:37 kernel: wpci3: 00:0b:6b:4d:22:b3 has associated
Dec 10 15:39:59 ntpdate[3527]: adjust time server 192.168.255.1 offset 0.0038
Dec 10 20:40:34 kernel: wpci3: 00:0b:6b:4d:22:b3 has disassociated
Dec 10 20:40:37 kernel: wpci3: 00:0b:6b:4d:22:b3 has associated
Dec 10 20:40:59 dropbear[3119]: exit after auth (admin): error writing
Dec 10 20:46:34 kernel: wpci3: 00:0b:6b:4d:22:b3 has disassociated
Dec 10 20:46:37 kernel: wpci3: 00:0b:6b:4d:22:b3 has associated
Dec 10 20:52:34 kernel: wpci3: 00:0b:6b:4d:22:b3 has disassociated
Dec 10 20:52:37 kernel: wpci3: 00:0b:6b:4d:22:b3 has associated
Dec 10 20:57:33 dropbear[3948]: Child connection from 10.10.1.189:36912
Dec 10 20:57:36 dropbear[3948]: password auth succeeded for 'admin' from 10.1
Dec 10 15:57:36 sshd: 10.10.1.189 logged in as admin
241:1
Close
Alt-X Exit CPU Load: 1.1% | XSCALE-WAR Edition v1.1.9 (build 1713)

fig 9: System log box

The Scripts Dropdown Submenu

The scripts submenu provides access to three areas: bandwidth management (via CBQ), firewall (packet filter) and port forwarding settings, and NAT (static and dynamic -- masquerading).

It also allows you to activate any changes made to scripts. You'll still need to do a File->Save to save the configuration between reboots, but the activate script command activates script changes immediately.

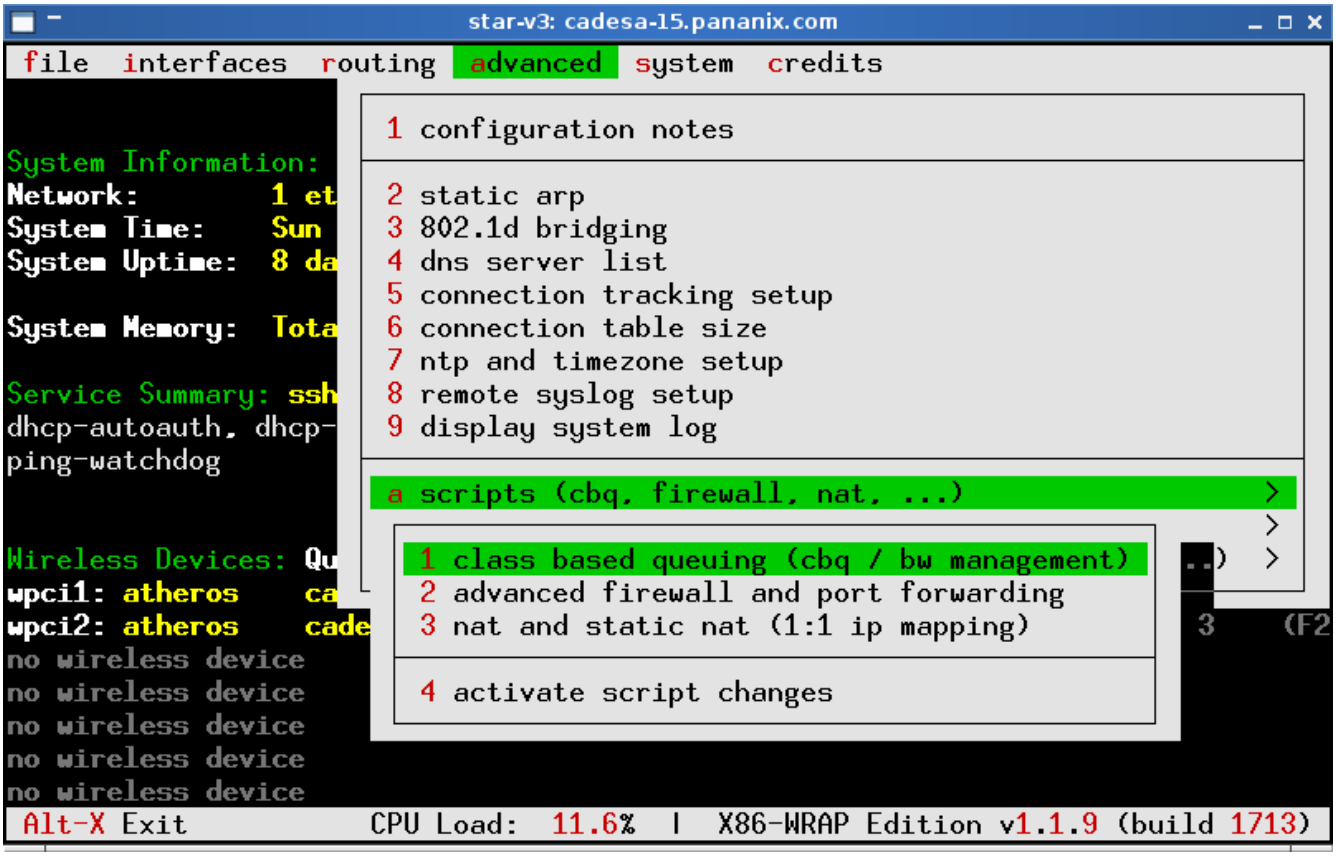


fig 10: Scripts dropdown menu

Class Based Queueing script

The CBQ script editor will allow you to set up bandwidth control and rudimentary quality of service for various classes of traffic/IPs. The script contains a number of examples, and in general handles setting up the root class for you.

While CBQ works well, if you need finer grained control, consider using either HTB (hierarchical token bucket) in a Linux router or AltQ (via pf) in *BSD. If you have many APs, there's something to be said for centralized bandwidth control and priority queueing using Linux or *BSD.

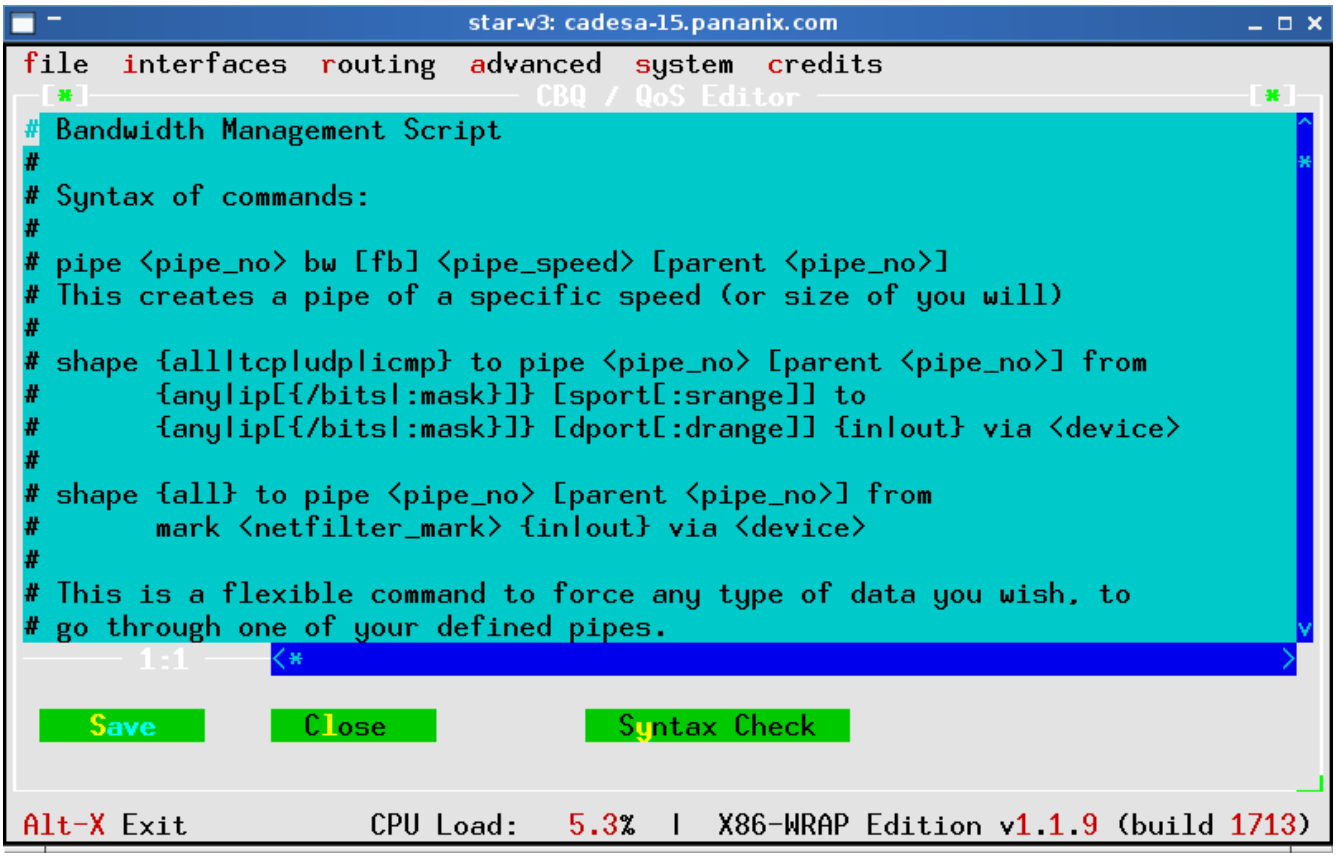


fig 11: CBQ and bandwidth editor

Advanced Firewall and Port Forwarding script

With the Advanced firewall script, you can allow or deny classes of traffic based on IP address (source or destination), port, or interface.

You can also port forward traffic on one interface to a system behind another interface based on port or IP address.

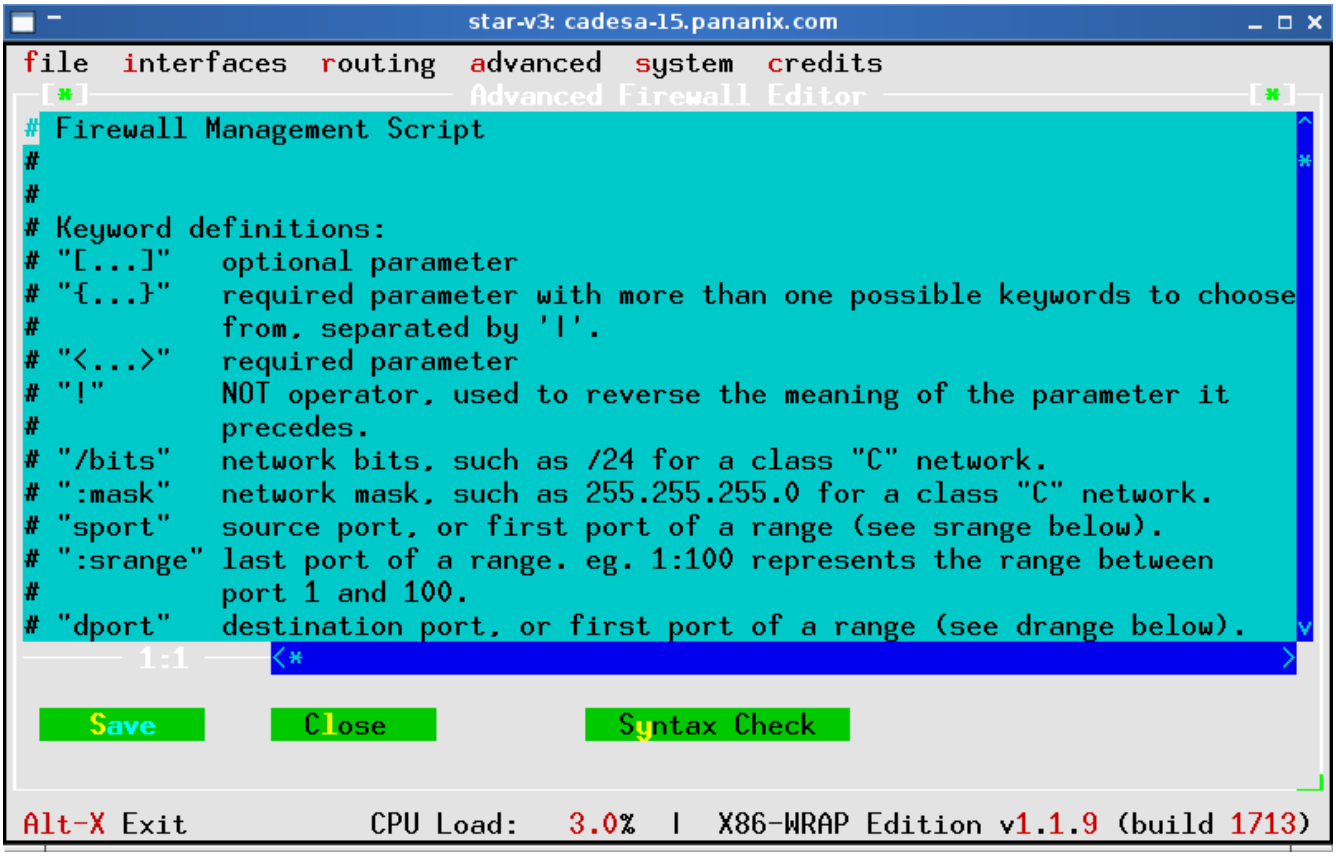
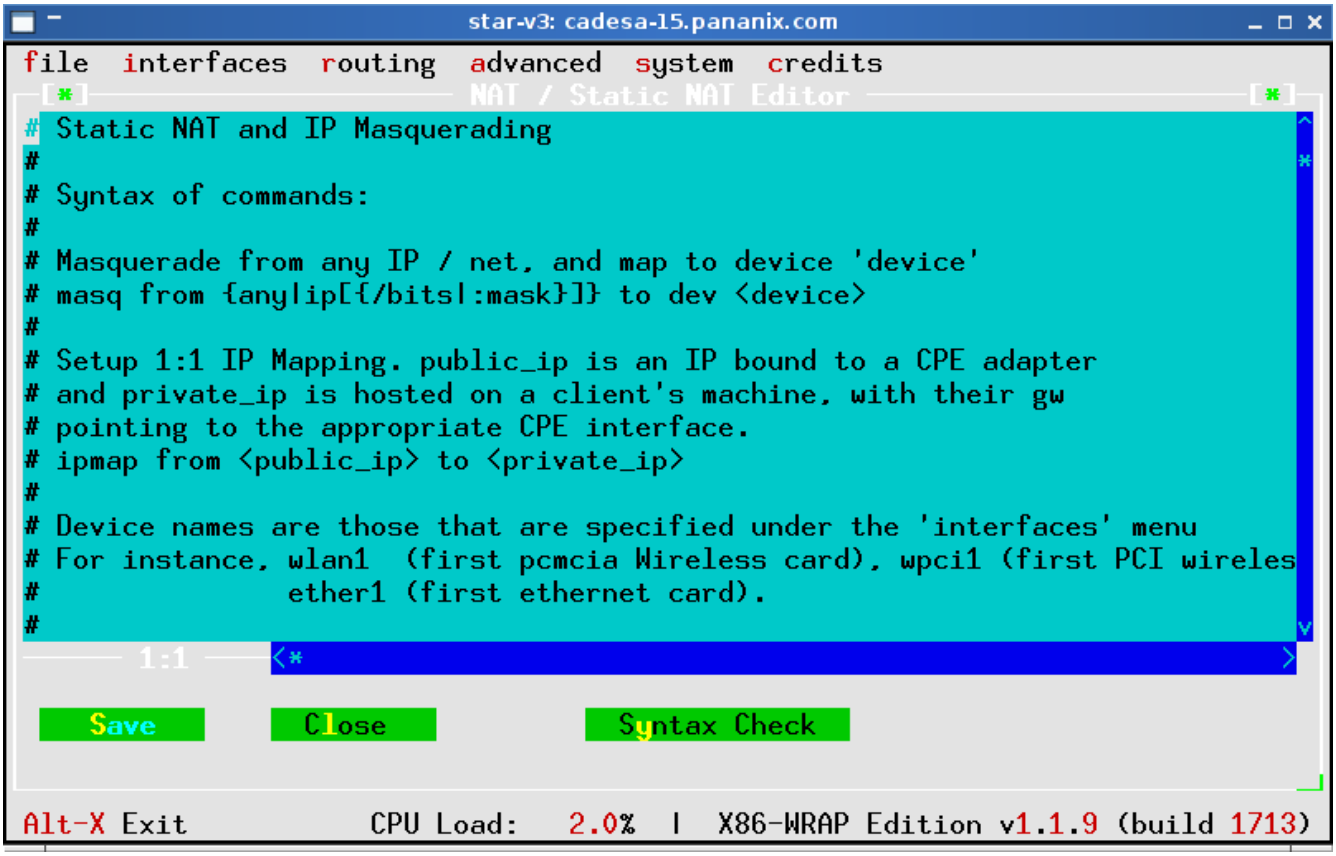

star-v3: cadesa-15.pananix.com
file interfaces routing advanced system credits
Advanced Firewall Editor
Firewall Management Script
#
#
Keyword definitions:
"[...]" optional parameter
"{...}" required parameter with more than one possible keywords to choose
from, separated by '|'.
"<...>" required parameter
"!" NOT operator, used to reverse the meaning of the parameter it
precedes.
"/bits" network bits, such as /24 for a class "C" network.
":mask" network mask, such as 255.255.255.0 for a class "C" network.
"sport" source port, or first port of a range (see srange below).
":srange" last port of a range. eg. 1:100 represents the range between
port 1 and 100.
"dport" destination port, or first port of a range (see drange below).
1:1
Save
Close
Syntax Check
Alt-X Exit
CPU Load: 3.0% | X86-WRAP Edition v1.1.9 (build 1713)

fig 12: Firewall and port forwarding script

NAT and Static NAT

The NAT and Static NAT script allows you to perform either of static 1:1 mapping, where a number of IPs behind one interface have a 1:1 mapping to other IPs on another interface.

But the most common usage by far is to perform “masquerading”, which is to map all private IPs behind one interface to a public IP on another interface. This anonymizes the systems on the private network and prevents direct access to them from the outside.


star-v3: cadesa-15.pananix.com
file interfaces routing advanced system credits
NAT / Static NAT Editor
Static NAT and IP Masquerading
#
Syntax of commands:
#
Masquerade from any IP / net, and map to device 'device'
masq from {any|ip[{/bits|:mask}]} to dev <device>
#
Setup 1:1 IP Mapping. public_ip is an IP bound to a CPE adapter
and private_ip is hosted on a client's machine, with their gw
pointing to the appropriate CPE interface.
ipmap from <public_ip> to <private_ip>
#
Device names are those that are specified under the 'interfaces' menu
For instance, wlan1 (first pcmcia Wireless card), wpci1 (first PCI wireles
ether1 (first ethernet card).
#
1:1
Save
Close
Syntax Check
Alt-X Exit
CPU Load: 2.0% | X86-WRAP Edition v1.1.9 (build 1713)
fig 13: NAT and Static NAT script

System Reports

The system reports dropdown menu allows you to choose between a report on CBQ traffic and a system information report.

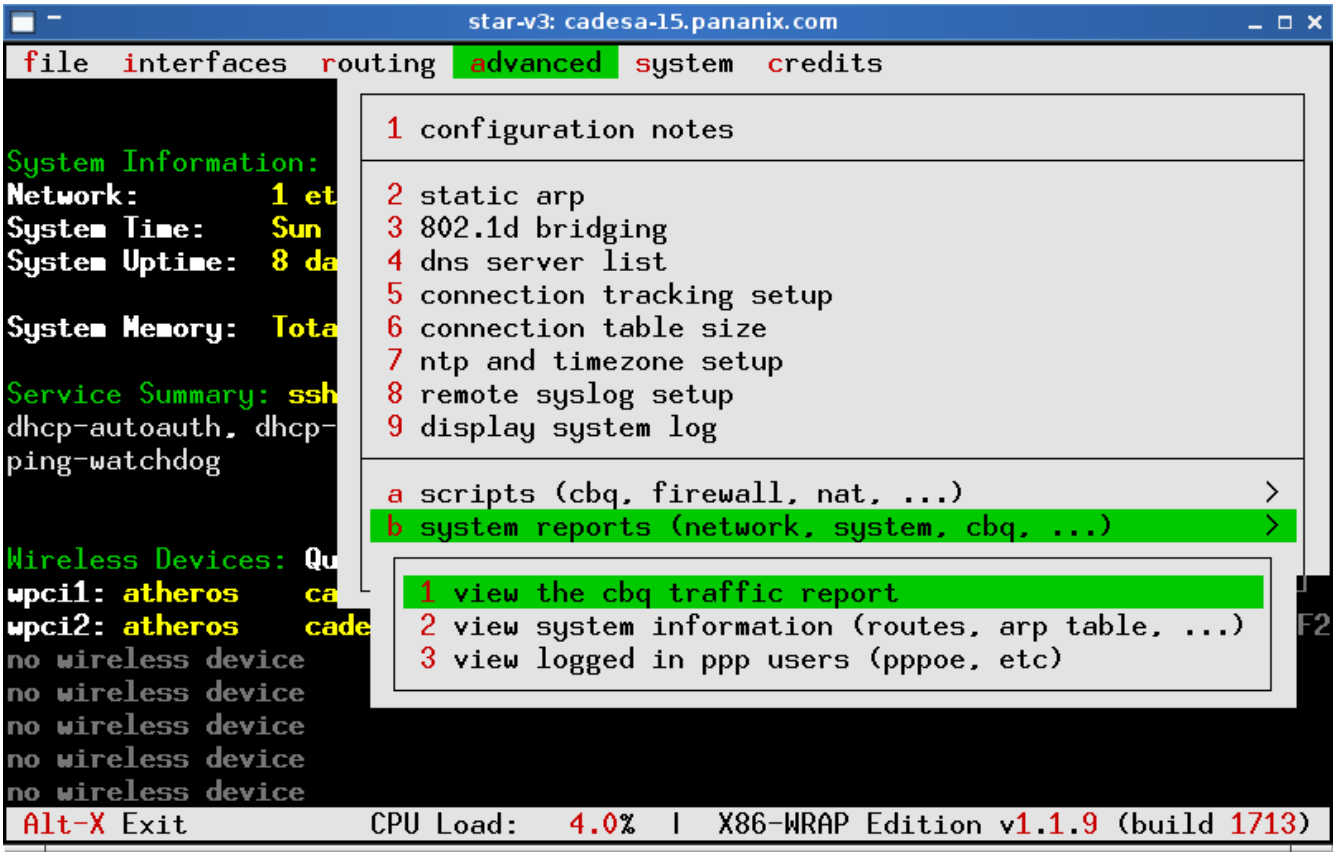


fig 14: System reports dropdown submenu

The CBQ Traffic Report

The CBQ traffic report will show you the amount of traffic transmitted and received in each individual queue. This will give you a good indication of traffic through this particular radio.

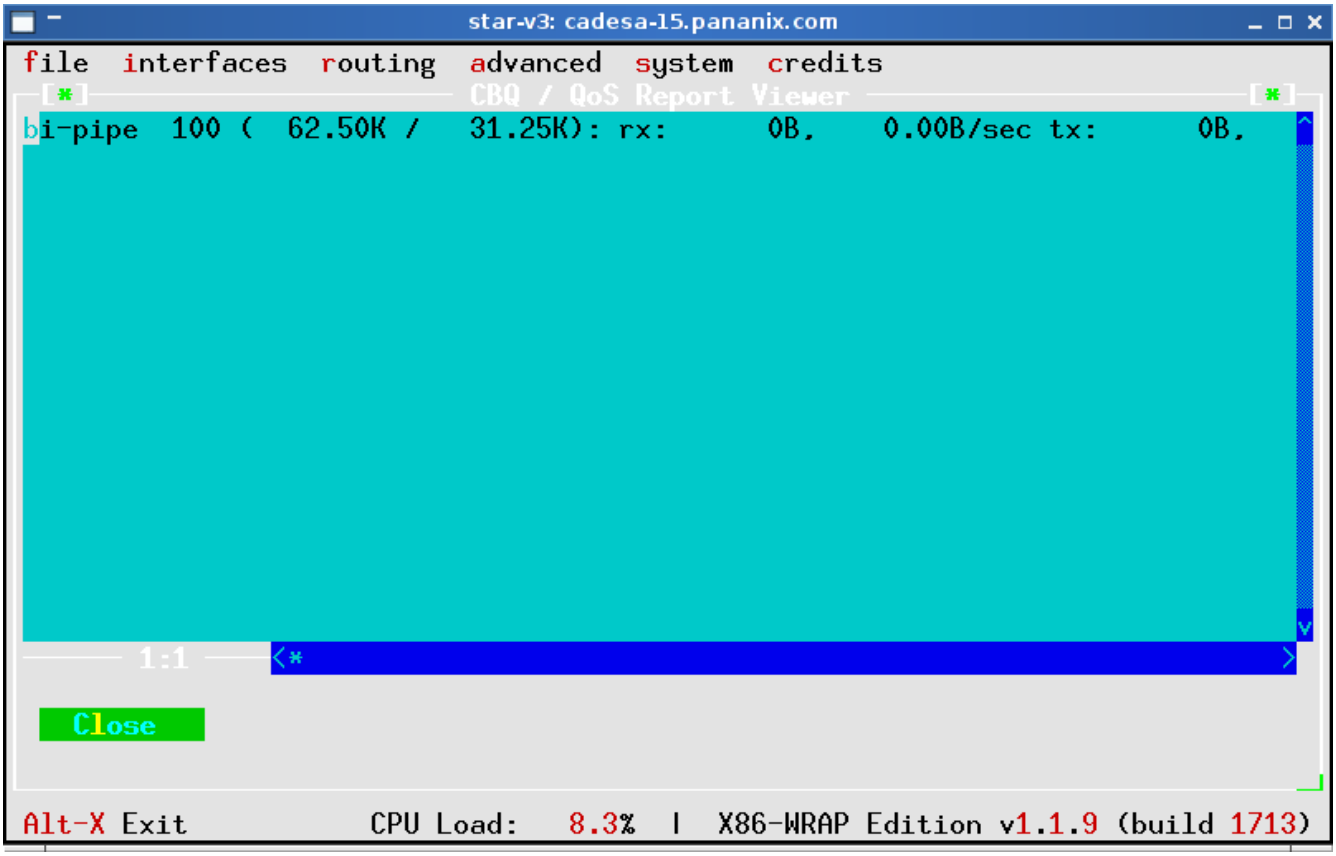

star-v3: cadesa-15.pananix.com
file interfaces routing advanced system credits
CBQ / QoS Report Viewer
bi-pipe 100 (62.50K / 31.25K): rx: 0B, 0.00B/sec tx: 0B,
1:1
Close
Alt-X Exit
CPU Load: 8.3% | X86-WRAP Edition v1.1.9 (build 1713)

fig 15: CBQ/QoS Report Viewer

View System Information

The system information report will show you what the system knows about itself and connected systems.

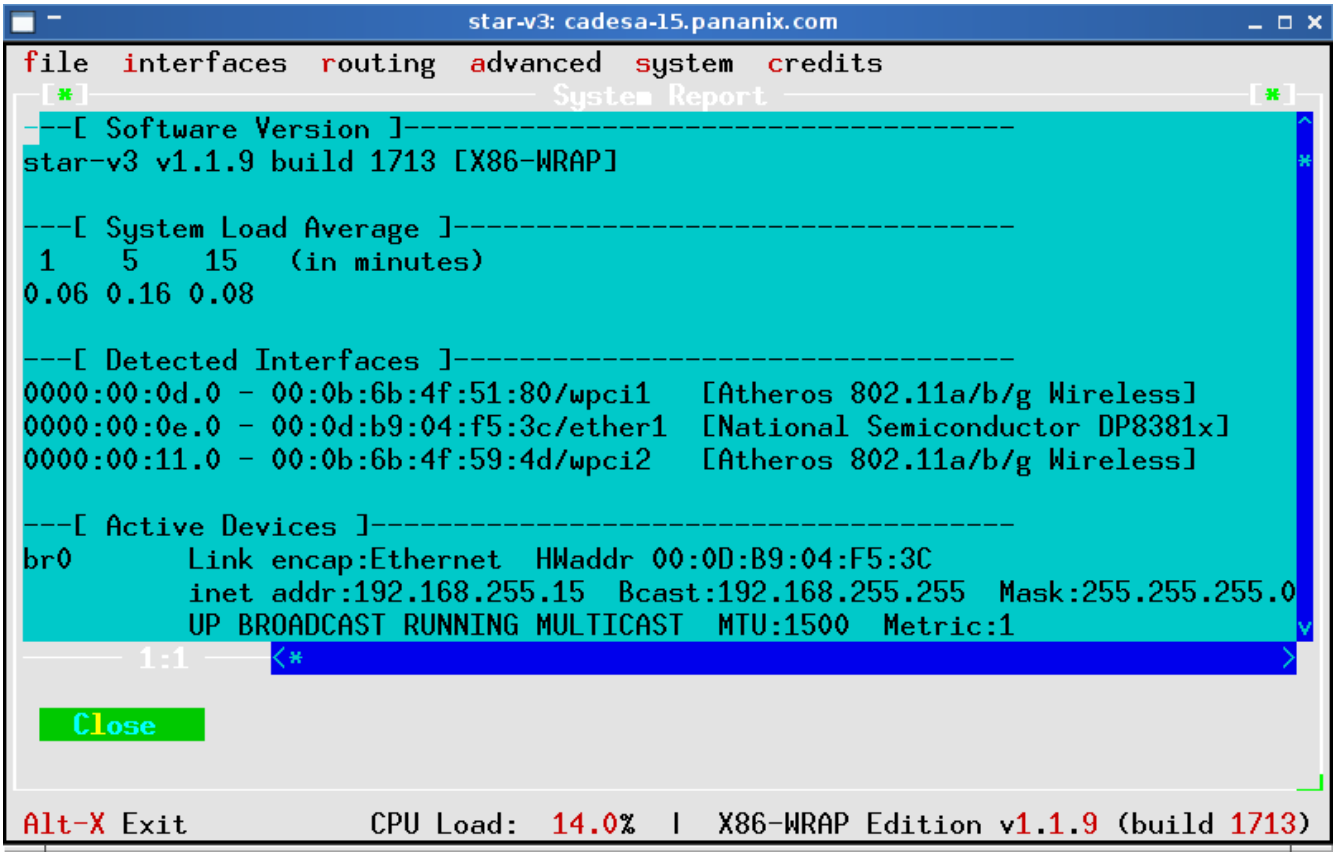

star-v3: cadesa-15.pananix.com
file interfaces routing advanced system credits
System Report
---[Software Version]---
star-v3 v1.1.9 build 1713 [X86-WRAP]
---[System Load Average]---
1 5 15 (in minutes)
0.06 0.16 0.08
---[Detected Interfaces]---
0000:00:0d.0 - 00:0b:6b:4f:51:80/wpci1 [Atheros 802.11a/b/g Wireless]
0000:00:0e.0 - 00:0d:b9:04:f5:3c/ether1 [National Semiconductor DP8381x]
0000:00:11.0 - 00:0b:6b:4f:59:4d/wpci2 [Atheros 802.11a/b/g Wireless]
---[Active Devices]---
br0 Link encap:Ethernet HWaddr 00:0D:B9:04:F5:3C
inet addr:192.168.255.15 Bcast:192.168.255.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
1:1
Close
Alt-X Exit
CPU Load: 14.0% | X86-WRAP Edition v1.1.9 (build 1713)

fig 16: System Information Report

Active PPP user list

If you are using PPP, your active users will show up in this list.

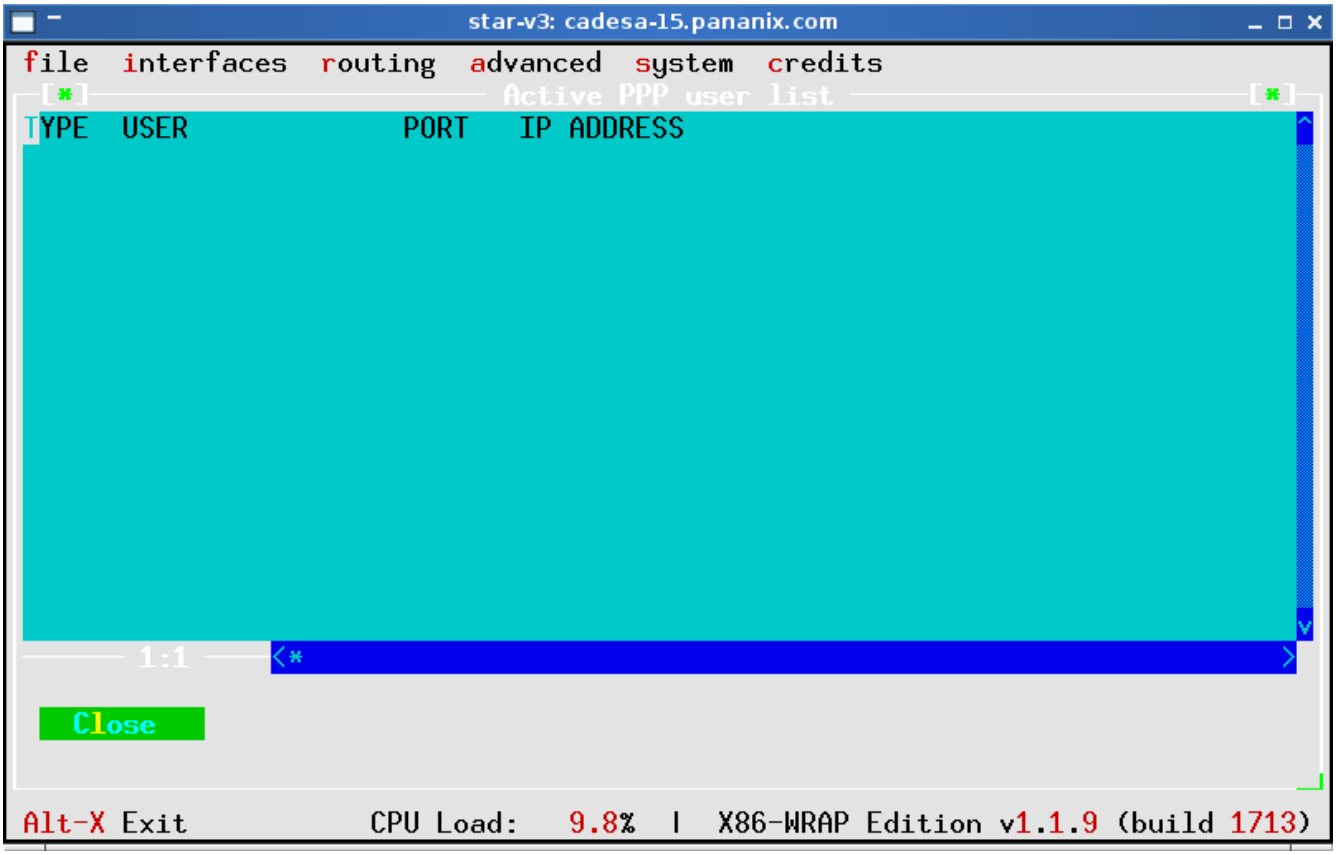

star-v3: cadesa-15.pananix.com
file interfaces routing advanced system credits
Active PPP user list
TYPE USER PORT IP ADDRESS
1:1
Close
Alt-X Exit CPU Load: 9.8% | X86-WRAP Edition v1.1.9 (build 1713)

fig 17: Active PPP User List

Network Utilities

The heart of network troubleshooting, this will probably be your first stop following complaints of network-related problems. This dropdown menu allows you access to ping, tcpdump, and throughput test.

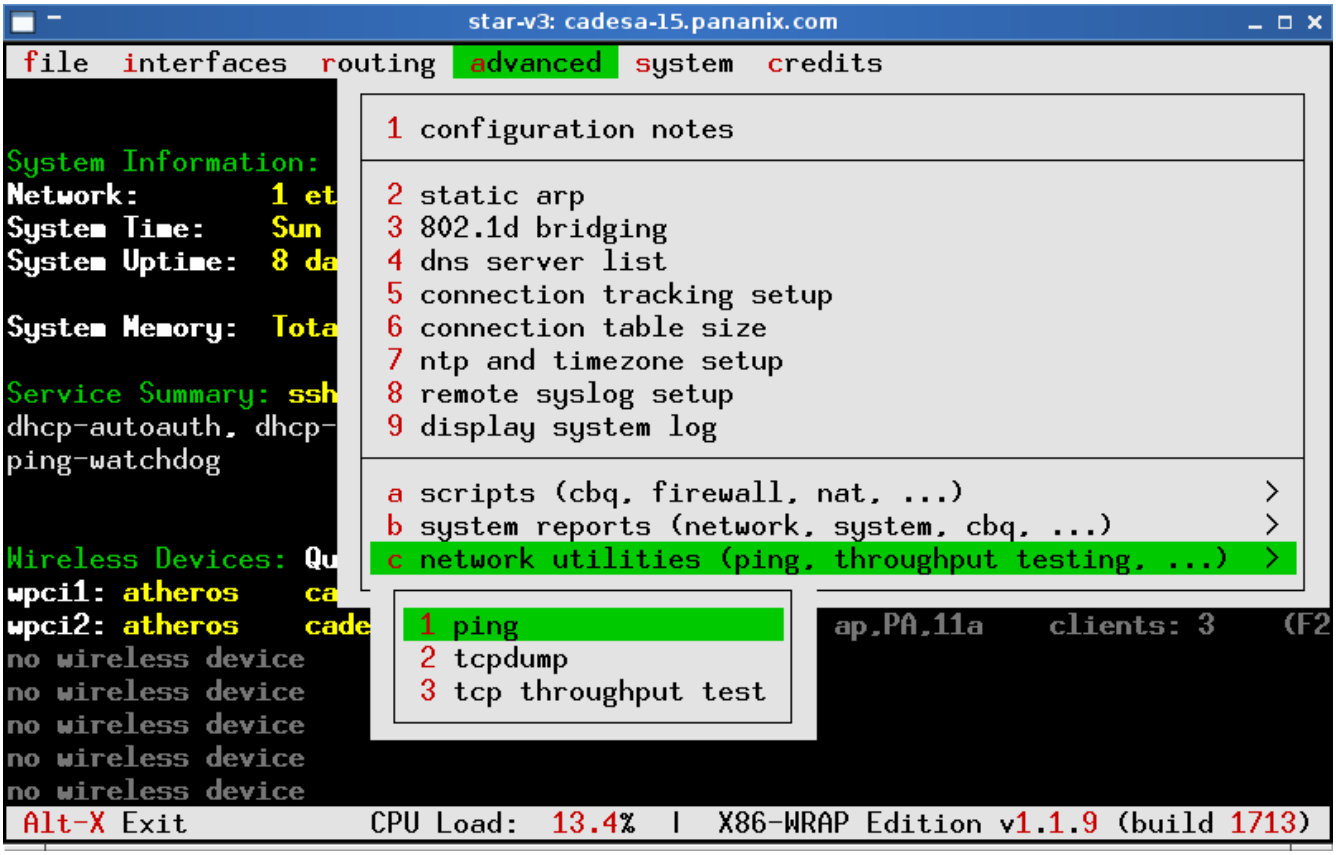


fig 18: Network Utilities dropdown submenu

Ping Utility

If you really want to know if you have a solid connection, this should be your first stop. The box will accept an IP or DNS hostname, but must have DNS configured (above) to use a hostname to ping.

By default, your packet size will be 56 bytes. This, combined with 28 bytes for the header gives you an 84 byte packet. Often, however, the problem is not small packets, but large ones.

If your MTU is the standard 1500, and you want to test if there is a problem with large packets, use a packet size of 1472. This should give you packets 1500 bytes (the MTU maximum). If these packets pass without loss, your link is good. Try running this ping all night as an acid test of a link.

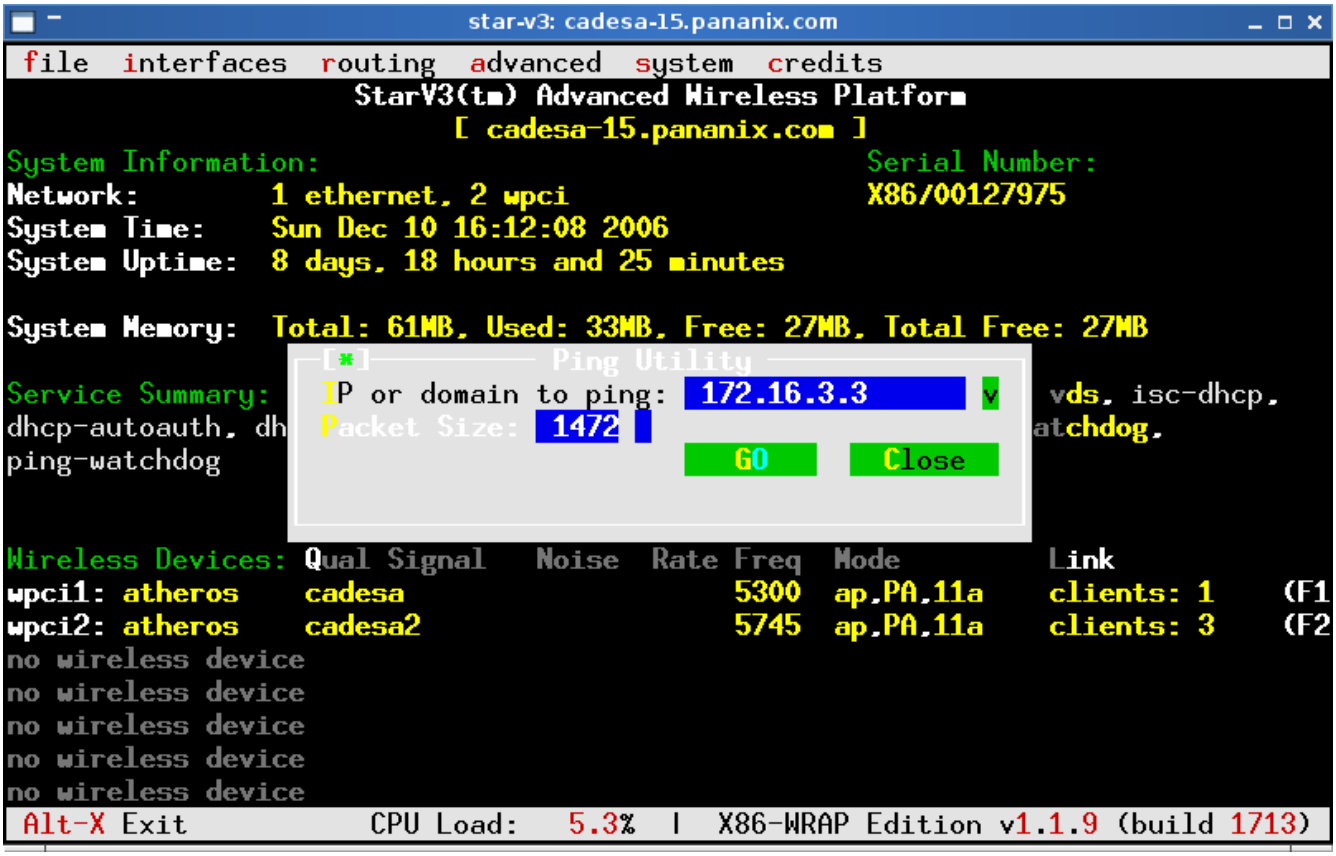

star-v3: cadesa-15.pananix.com
file interfaces routing advanced system credits
StarV3(tm) Advanced Wireless Platform
[cadesa-15.pananix.com]
System Information:
Serial Number:
Network: 1 ethernet, 2 wpci
X86/00127975
System Time: Sun Dec 10 16:12:08 2006
System Uptime: 8 days, 18 hours and 25 minutes
System Memory: Total: 61MB, Used: 33MB, Free: 27MB, Total Free: 27MB
Ping Utility
IP or domain to ping: 172.16.3.3
Packet Size: 1472
GO
Close
Service Summary:
vds, isc-dhcp,
dhcp-autoauth, dh
atchdog,
ping-watchdog
Wireless Devices: Qual Signal Noise Rate Freq Mode Link
wpci1: atheros cadesa 5300 ap,PA,11a clients: 1 (F1
wpci2: atheros cadesa2 5745 ap,PA,11a clients: 3 (F2
no wireless device
no wireless device
no wireless device
no wireless device
no wireless device
Alt-X Exit CPU Load: 5.3% | X86-WRAP Edition v1.1.9 (build 1713)

fig 19: Ping Utility box

Ping response

The response box will show you the IP being sent ICMP ping packets, the packet number, the size, the round trip time (RTT), and the percent loss. You should normally not lose packets.

If you calculated 1500 byte packets by subtracting the 28 byte header, but see packets of size 1528 being sent, you probably are running a VLAN and didn't compensate. If packets don't pass, somewhere along the route you have an interface that has a 1524 byte limitation. Go back, reduce your MTU to 1400 and try again, using 1344 bytes.

Lowering your MTU will affect throughput on large transfers, but is better than no transfer.

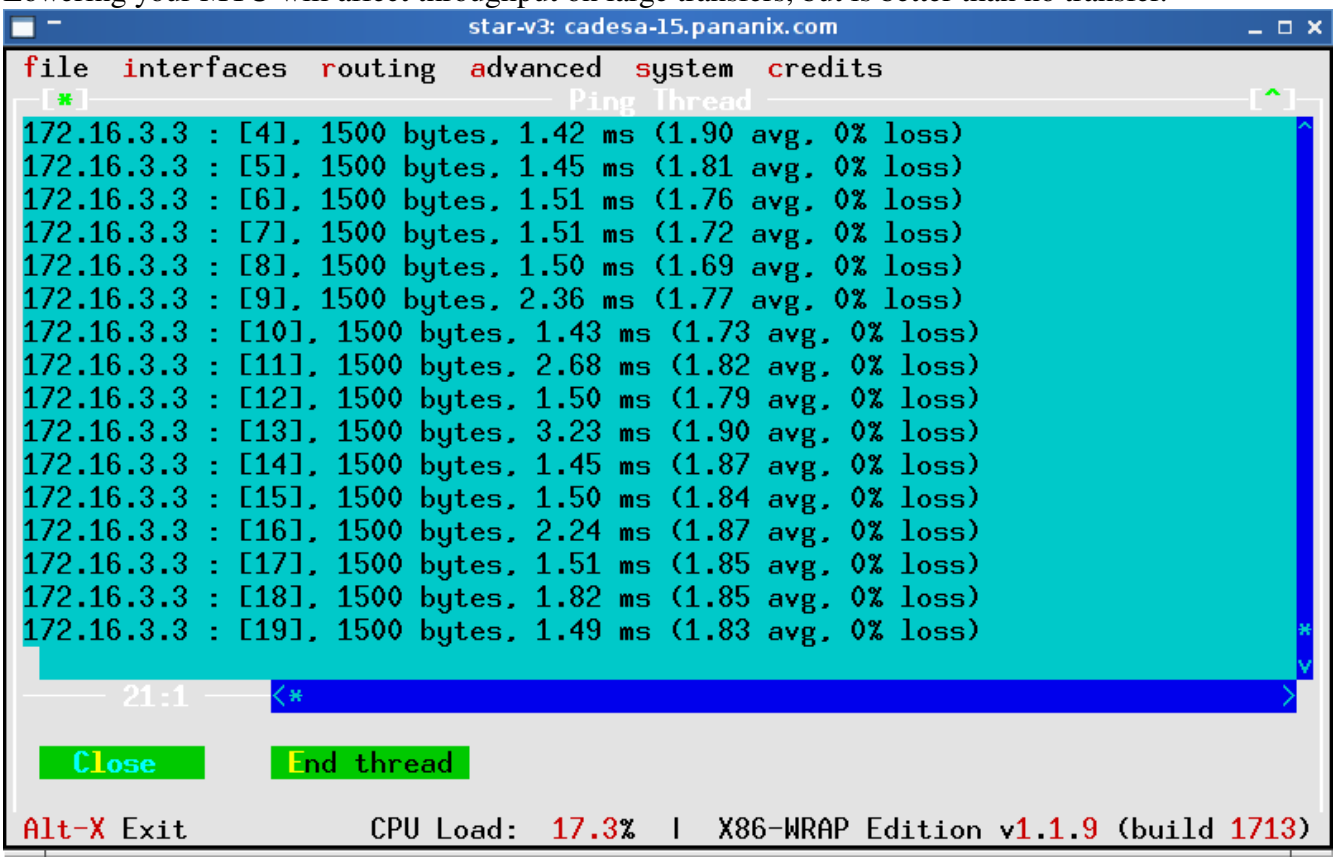

star-v3: cadesa-15.pananix.com
file interfaces routing advanced system credits
Ping Thread
172.16.3.3 : [4], 1500 bytes, 1.42 ms (1.90 avg, 0% loss)
172.16.3.3 : [5], 1500 bytes, 1.45 ms (1.81 avg, 0% loss)
172.16.3.3 : [6], 1500 bytes, 1.51 ms (1.76 avg, 0% loss)
172.16.3.3 : [7], 1500 bytes, 1.51 ms (1.72 avg, 0% loss)
172.16.3.3 : [8], 1500 bytes, 1.50 ms (1.69 avg, 0% loss)
172.16.3.3 : [9], 1500 bytes, 2.36 ms (1.77 avg, 0% loss)
172.16.3.3 : [10], 1500 bytes, 1.43 ms (1.73 avg, 0% loss)
172.16.3.3 : [11], 1500 bytes, 2.68 ms (1.82 avg, 0% loss)
172.16.3.3 : [12], 1500 bytes, 1.50 ms (1.79 avg, 0% loss)
172.16.3.3 : [13], 1500 bytes, 3.23 ms (1.90 avg, 0% loss)
172.16.3.3 : [14], 1500 bytes, 1.45 ms (1.87 avg, 0% loss)
172.16.3.3 : [15], 1500 bytes, 1.50 ms (1.84 avg, 0% loss)
172.16.3.3 : [16], 1500 bytes, 2.24 ms (1.87 avg, 0% loss)
172.16.3.3 : [17], 1500 bytes, 1.51 ms (1.85 avg, 0% loss)
172.16.3.3 : [18], 1500 bytes, 1.82 ms (1.85 avg, 0% loss)
172.16.3.3 : [19], 1500 bytes, 1.49 ms (1.83 avg, 0% loss)
21:1
Close
End thread
Alt-X Exit
CPU Load: 17.3% | X86-WRAP Edition v1.1.9 (build 1713)

fig 20: Ping response box

tcpdump Utility box

The tcpdump utility will allow you to see traffic passing through the chosen interface. Note that if you choose a bridged interface, you'll see a lot of traffic not destined for the chosen interface.

All valid tcpdump expressions can be used (read the man page for a relatively complete list).

You can choose to resolve IP names, but only if you have enabled DNS (above). Be aware that this will slow down your dump and cause you to miss packets because they will be dropped. Only resolve IP names if you really need to.

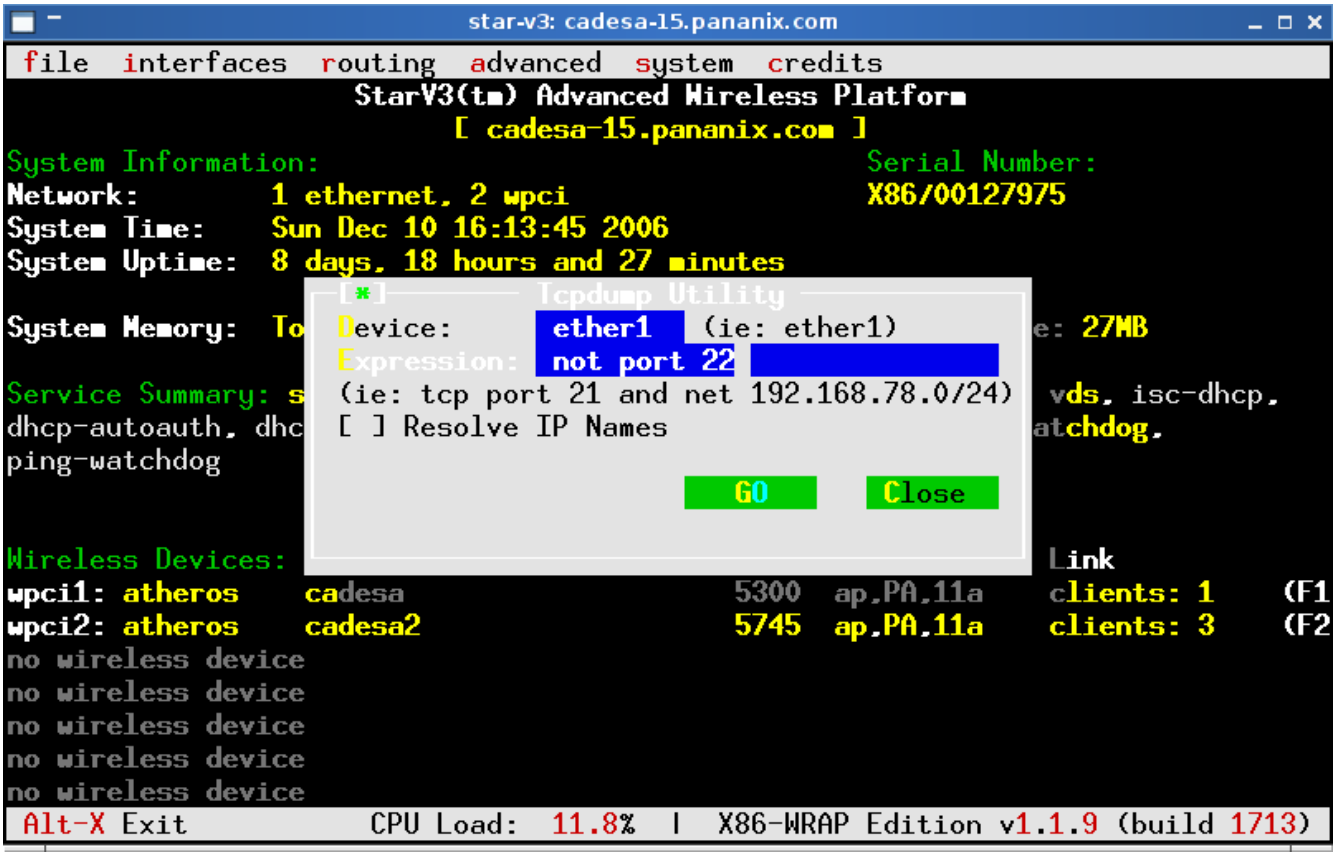


fig 21: tcpdump utility box

tcpdump response box

The tcpdump response box will show you the normal, non-verbose output showing a summary of the headers. How to read this dump is beyond the scope of this text, but the man page is an excellent place to start.

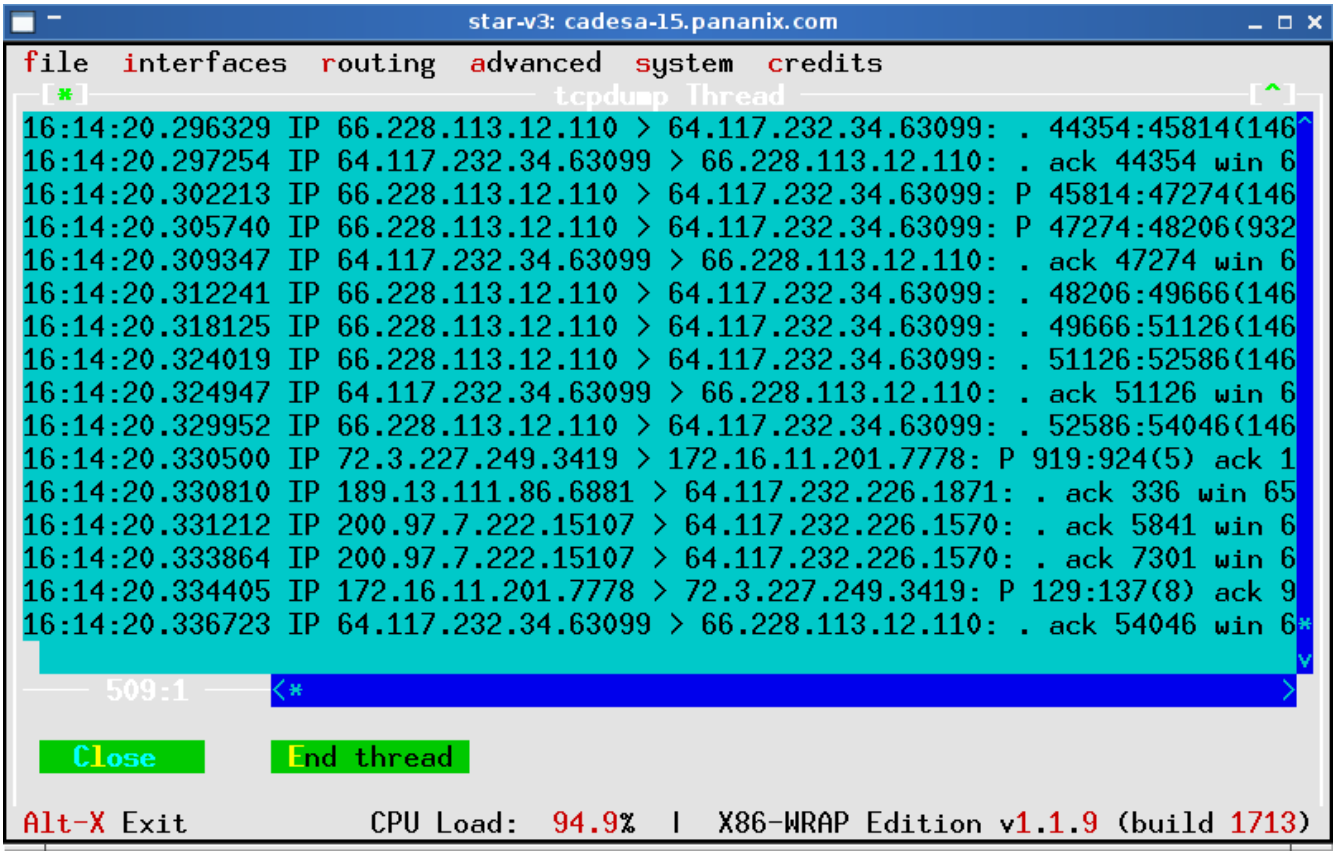


fig 22: tcpdump reponse box

Throughput Test Box

If you're curious how capable your link is, this is a good place to start. One word of caution, this test is extremely detrimental to network traffic, and should not be used on a production link (unless of course you want to hear a lot of screaming about a slow connection from users).

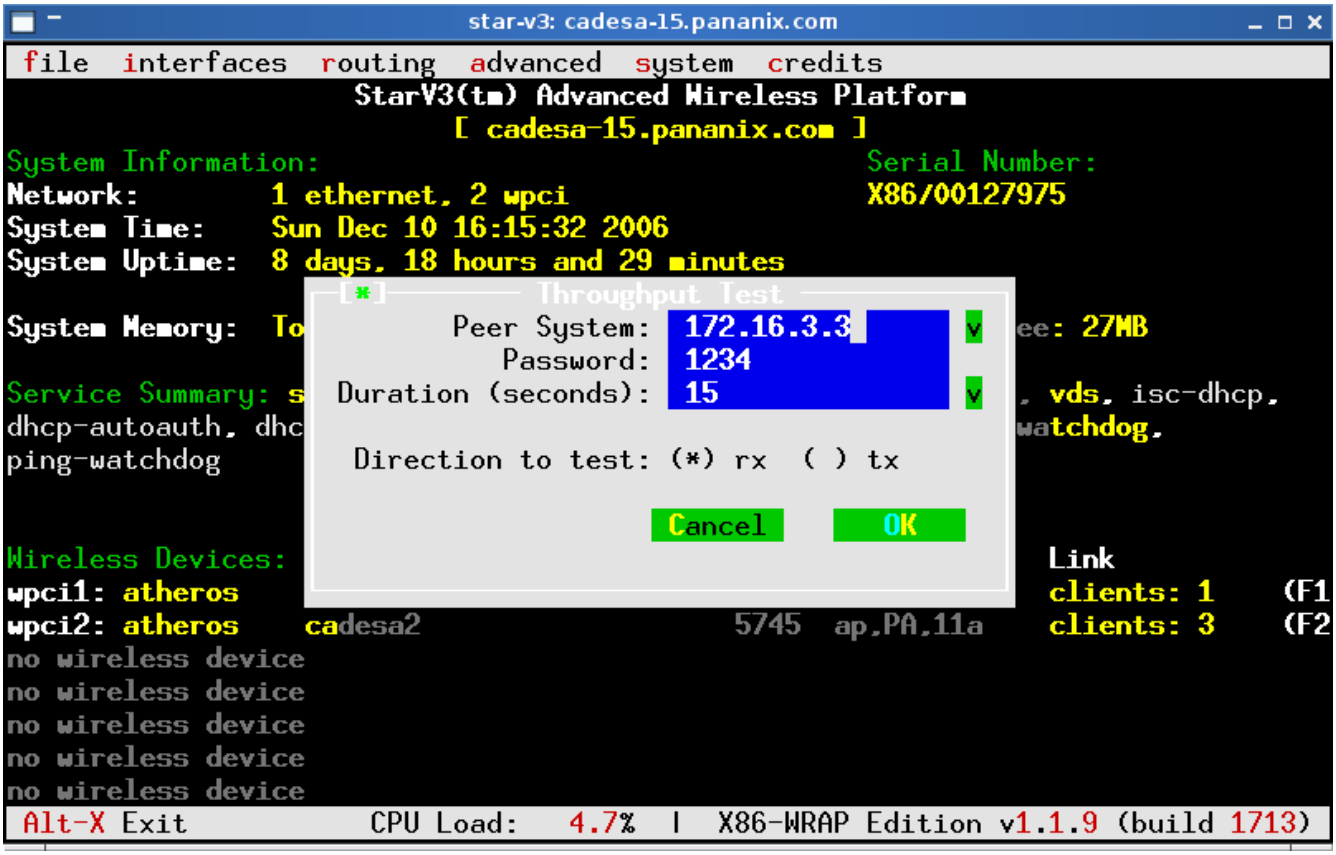


fig 23: Throughput Test box

Throughput Test Response Box

The throughput test response box will update every second until the test ends. Throughput is measured in K bytes per second. To find bits per second, multiply the number by 8.

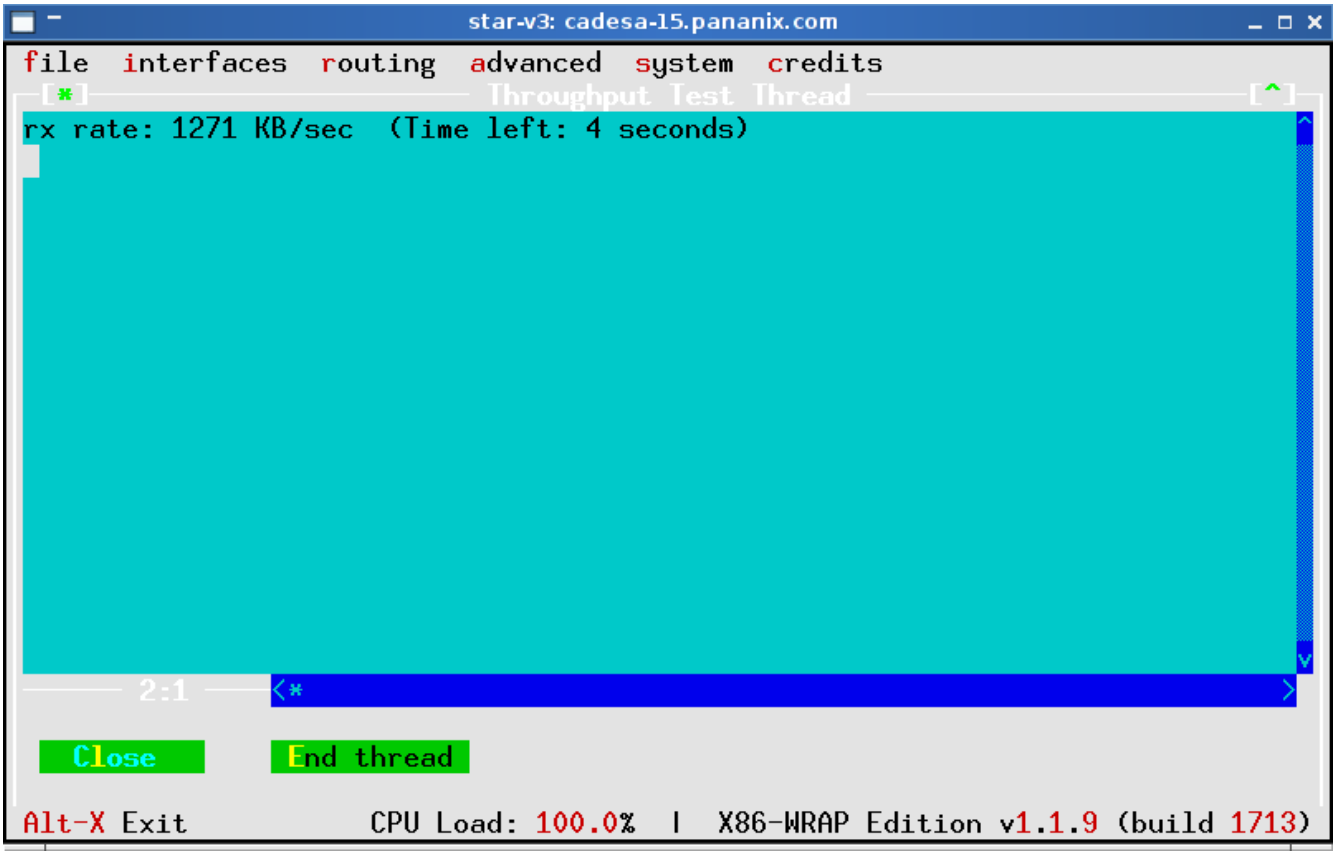


fig 24: Throughput Test response box

Chapter 7

Configuration, Upgrades, Tips and Tricks

StarOS comes with a command line utility called starutil which will allow you to perform a range of operations on a system. This includes but is not limited to, uploading new software, up and down loading the radio's configuration, rebooting remotely, etc.

The starutil utility is available from www.staros.com for Windows and Linux. BSD systems can run the Linux binary if that option has been selected during system setup.

starutil

If you run the starutil command without any arguments, or with an argument of -?, h, or –help, you'll receive a usage display(see fig 1). Note: not all available starutil commands will work on a StarOS V3 system.

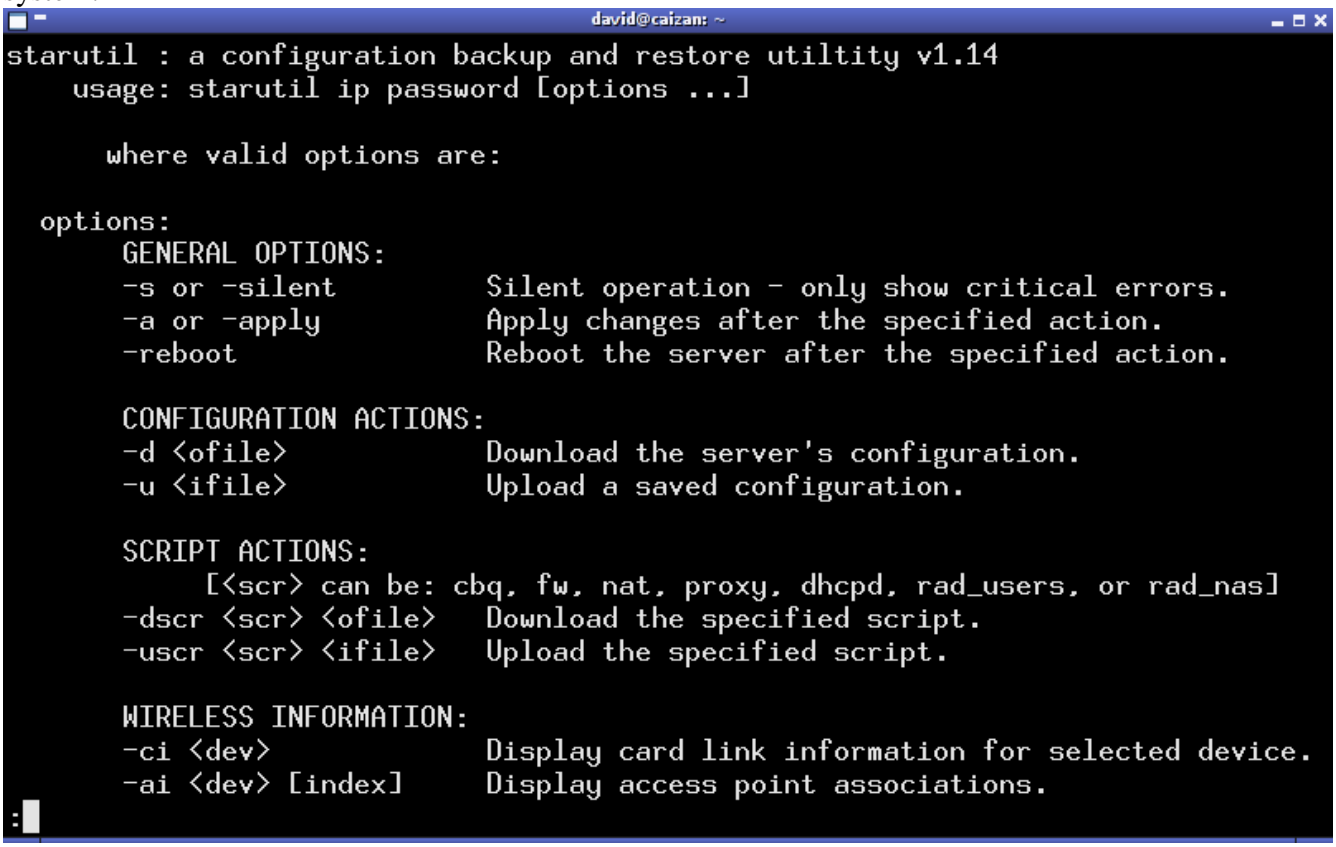

david@caizan: ~
starutil : a configuration backup and restore utiltity v1.14
usage: starutil ip password [options ...]
where valid options are:
options:
GENERAL OPTIONS:
-s or -silent Silent operation - only show critical errors.
-a or -apply Apply changes after the specified action.
-reboot Reboot the server after the specified action.
CONFIGURATION ACTIONS:
-d <ofile> Download the server's configuration.
-u <ifile> Upload a saved configuration.
SCRIPT ACTIONS:
[<scr> can be: cbq, fw, nat, proxy, dhcpd, rad_users, or rad_nas]
-dscr <scr> <ofile> Download the specified script.
-uscr <scr> <ifile> Upload the specified script.
WIRELESS INFORMATION:
-ci <dev> Display card link information for selected device.
-ai <dev> [index] Display access point associations.
:

fig 1: partial starutil usage screen display

The three most important options you'll use include the -d to download the radio's configuration, the -u to upload the configuration to a new radio, and the -f to upload a file to the upgrade buffer. You may also find the -reboot option useful for radios reluctant to allow you to login for whatever reason.

Saving and restoring configurations

To save a radio's configuration, use the following command:

starutil <IP_of_radio> <password_for_admin_user> -d <filename>

which will look like this:

starutil 192.168.1.1 1234 -d radio1.dat

To load a radio with a known good configuration, run the following command:

starutil <IP_of_radio> <password_for_admin_user> -u <filename>

which looks like this:

starutil 192.168.1.1 1234 -u radio1.dat

You can add the -a to have the system activate the file upon successful upload.

Once a configuration is uploaded, you can issue:

starutil 192.168.1.1 1234 -reboot

Note that, if the uploaded configuration file contained a password, you'll have to substitute that password for 1234.

Which brings up those things that are saved within the configuration file (or more importantly, what's not). Basically, after uploading a configuration file to a new radio, that radio is a clone of the other with the exception of the license key. That key will not be overwritten.

It is prudent to install the license key and reboot prior to attempting to upload the configuration.

For those of you who like to “automate” saving of configurations, I have cron run a script weekly to save radio configurations (in case I made a change I forgot to record to a new configuration file). The crux of this script is this line which may be run on a command line as is:

```
for i in `cat radios.txt`; do ./starutil $i my_passwd -d $i.`date +%y%m%d`.dat;
done
```

I keep a list of radio IPs in the file radio.txt, one IP per line. I also keep the starutil utility in the directory with the radio.txt file and the dat configuration files.

Upgrading

Upgrades to the StarOS radios can are a two-step process. First, the upgrade file needs to be uploaded to the radio:

starutil 192.168.1.1 1234 -f vncOs-1.1.2-1421.X86-WRAP.pkg

This will upload the new configuration into the upgrade buffer. Now you will need to log into the radio and select System->upgrade firmware. You will get warnings about the hazards of upgrading, i.e., that your radio may not work for whatever reason. Once you've upgraded the firmware, a reboot will see

you running the new version. If you do not continue the upgrade, the radio will continue to boot from the old image.

Starutil has a number of other commands, but some of these commands are not available to version 3 of StarOS, at least not yet. For example, getting the status of wireless connections is not supported.

Tips and Tricks

Some of you may be interested in some quick tips and tricks. If you have a favorite tip or trick, please let us know in the forum.

You can use snmp in a number of ways if you have it turned on. Some of you will be familiar with the UNIX command line snmpwalk to get information from your systems for statistical purposes, or just to see if the system is up. One quick tip is to create a file with the IP of each radio (radio.txt) and run the following from a UNIX command line on a system with snmpwalk installed:

```
for i in `cat radios.txt`;do x=`snmpwalk -c public -v 2c $i sysUpTime`; y=`echo $x| cut -d: -f4-6`;echo $i $y;done
```

Note that the above is one line. Using this it's easy to see at a glance when a radio has recently reboot. The radio.txt file and command line can be easily modified to provide InOctets/OutOctets on a particular interface, or any of a number of other parameters that change over time. Saving this information to file or database makes it easy to gather whatever statistics you want. Graphs are easily created using rrdtool.

Chapter 8

Wireless Practices

This chapter will focus on a number of pitfalls and ways to ensure you put up good links. Some things will be glossed over a bit. For example, we'll discuss antenna selection, but there's little sense in reproducing hundreds of pages of HAM antenna theory. We will, however, cover in depth how to set up long distance links (the most difficult). So hold on to your hats.

Your radio

We've covered the basics (and more) of configuring your radio. But you're not quite ready to install it on a tower. Before donning your safety belt or climbing harness, let's take a good hard look at how you're going to power the radio.

Most of us are using POE. The WRAP cards are capable of taking power from the Ethernet cable or from a plug directly to the board. When using POE, you must ensure two things: first, that your power supply provides adequate amperage. What works on the bench may not work well under load. Your first clue will be unexplained reboots during peak traffic loads. And second, keep your POE runs short to avoid power losses on the cables. Powering the POE injectors directly from a marine deep-cycle battery will ensure you have plenty of power available for longer cable runs.

It may be to your advantage to install a NEMA 4 enclosure mid-tower with a small switch and large POE adapters inside and only bring power from the ground to the box (see also Your tower, below).

Your tower

This cannot be stressed enough. You must ensure adequate grounding for your tower and all systems on it.

The tower itself should be grounded at each leg. You'll also want to have either a lightning rod with a sharp point or preferably a static discharge device like the bristle brush looking devices at the top of the tower.

No silver bullet exists to prevent lightning strikes and the damaging effects of ESD (electro-static discharge). In fact, there are various schools of thought on the subject. But the advice this book will give you is to ground <u>everything</u> as well as you can to a common ground. Take care not to end up with a split ground. A split ground is two or more ground points at different potentials due to the time it takes a lightning discharge to travel from one ground rod to the other (travel times are different through different mediums).

The purpose of the lightning rod or brushes is not to attract lighting (as the name lightning rod suggests), but rather to discourage the formation of a “leader” by dissipating an electrostatic potential into the passing cloud slowly (thus the reason for a well-sharpened point on your lighting rod). The more potential dispersed prior to formation of a leader (that first stroke of lightning), the better. Then, any leader that does form will be much weaker potential. It is crucial that whatever device you're using

has a clear, unobstructed path to the best ground you can afford to put in.

So what constitutes a good ground and a clear unobstructed path? Remember when dealing with lightning, that we're talking about static DC discharge of extremely high voltages. Also understand that while lightning is DC, it acts like high frequency AC (basically radio frequency – RF – signal). That means that what we install has to conform to good radio signal passing procedures. If you aren't convinced lightning acts like RF in a circuit, turn on an AM radio during a storm and you can hear strikes miles away.

High frequency RF travels over, not through, a conductor. The more surface area you present, the better. Flat braid or pipe strap works better than round conductors. Along those same lines, multi-strand conductors work better than solid conductors (more surface area). Arc-welding cable, while expensive, makes an excellent conductor.

The pathway for carrying lightning to ground should be as straight as possible. If you make one or more 360 degree wraps in a cable (the smaller the diameter, the greater the effect), you will make a choke or coil that will impede the flow of RF energy. In fact, one lightning dissipation device is made with 10 turns of ½ inch square copper bar. One end is sharpened and functions as the lightning rod, the other end is tied to ground. Lightning striking this rod takes a great deal of time (relatively speaking) to pass through this coil and is reduced from thousands of volts to mere hundreds and runs to ground safely. But use of a coil like this runs the risk of side flashing (lightning arcing through any insulator to other parts of the tower structure or cables running parallel to the ground lead) until after it has passed through the coil.

Whenever possible, put your systems 5 feet or more below the top of the tower. This is not always possible, but systems/antennas at the top of the tower will be at greatest risk. Ensure you have good, well-grounded lightning protectors just outside the radio enclosure (which should be made of metal, not plastic). Never put a lighting protector inside a metal box. And use grounded POEs. The most commonly available POEs are not grounded, but for outdoor cable runs, this is important. Your choice of lightning protectors is important as well. Gas discharge tubes will react faster, although the discharge tubes will need replacing more often.

Cables

Ethernet/POE cables

Ethernet cables used outdoors should be the gel-filled outdoor rated cable. Using indoor cable outdoors will work – for a while. But this cable is subject to degradation from the sun's ultra-violet rays and will need frequent replacing. Doing it right the first time will save doing it over later.

Many folks worry about Ethernet cable picking up EMP (electro-magnetic pulse) from a lightning strike and damaging Ethernet ports on WRAP cards and switches. This is usually an unfounded worry. Ethernet ports damage first because of all the electronic equipment, they have the lowest tolerance to power surges. Most electronic equipment is rated at 1000v. Ethernet ports are rated at 100v. While the standards have changed, it will take some time to get these newer chips deployed. Damaged Ethernet ports are usually damaged because they became an alternate ground path and lacked grounded POEs to

protect them. All that said, Ethernet cables can pick up EMP when strung like a clothesline from a client on a post in the yard to the house. Long horizontal Ethernet cable runs should be buried.

Antenna cables

Most folks deploying detached antenna systems opt to build their own antenna cables. After all, how hard can it be? Unfortunately, many also opt not to purchase the proper equipment to build the cables. While a crimper is essential, most believe proper cable strippers are not.

Any nick or cut in the center conductor will alter the characteristics of the cable. Many of you will have heard at one time or another someone else on your telephone line. This is a result of near-end crosstalk from a telephone cable that has nicks or gouges in the wires. The effects in the GHz range are worse and include excess reflected power and poor impedance match. Ensure your center conductor is not damaged.

Some folks also feel that the mechanical connection made by the crimpers used to crimp the pin to the center conductor is not good enough, so they solder the tips on. While this may not be a bad idea, using a too hot iron or the wrong solder is much worse. If you absolutely must solder your connections, use a maximum 60 watt iron and resin core solder, not acid core solder. Resin core is for circuit boards, acid core is for plumbing, and we're not plumbers.

When you're ready to connect your cables, you must ensure no moisture can enter the connectors. For years most of us used 3M 130 or similar tape. This is high voltage rubber tape, not the plastic electrical tape (if you are using that, throw it out). Some folks have also used a similar rubber compound that comes in rolls or sheets and can be formed around the connector. But the best thing to use to keep moisture out of connectors is STUF, an insulating dielectric compound. Just a small squirt into the area of the center connector and you can forget moisture problems.

Finally, when installing your LMR-400 or LMR-240 cables, ensure your tie wraps are not so tight they deform the cable. The electrical characteristics of the cable are altered if the distance between the center conductor and the shielded braid is changed.

While some operators swear by the gel-filled LMR cable (LMR-###DB, the DB standing for direct burial), as long as the outer covering is not damaged, water should not be a problem. Non-gel cable should not be run underground or on the ground where it may sit in water. And installed cable should never be removed and reinstalled at another site. Discard old cable, it's cheaper to buy new than endure problems with old cable.

Antennas

If you glossed over any of the above as unimportant, please pay attention to this part. The absolute most important part of your radio system is the antennas. You must choose the appropriate antennas for the link you wish to make. All else being equal, a 25 dbi grid antenna will allow you to communicate twice as far on half the power as a 22 dbi grid will. In general, you'll be better off with two 17 dbi sector antennas and a splitter/combiner than with a 12 dbi omni. First you'll be able to focus your (usually narrow) horizontal band better, but secondly, and more importantly, you'll be able to hear weak

signals much better.

In the field, nothing beats a good pair of ears. I've seen folks install wireless systems, find the link is weak, and decide the best thing to do is slap an amp on. While their signal improved, for the marginal improvement, they added greatly to the ambient noise, probably interfered with a like-minded operator who will also just slap an amp on, and no one wins. When you use an amplifier, you amplify noise as much as you do signal. You can also cause signal distortion through signal clipping at the receiver when it is overdriven. These radios are designed to work well with low signal levels.

Choosing your antenna correctly is nothing more than understanding how radio works and applying calculations to ensure your link will have good signal levels before you install.

If you are unsure of how important antennas are, try running your calculations (see Calculations, below) using different gain antennas and at different power levels. This should give you some idea. For example, a 6 dbi antenna listening to a 4 watt signal will receive a signal of -80db at 3.2 miles away. But change that to a 30 dbi antenna listening to the same 4 watt signal and you will receive -80db at 50 miles. Assuming receiver sensitivity of -86 in both cases, each has an SNR of 6db. If this paragraph made little or no sense to you, keep reading.

Calculations

Before performing your calculations, there are a few terms you should understand. These will be explained below. They include Fresnel zone, SNR, and more.

Environment

If you are using DSSS (direct sequence spread spectrum) technology (most 2.4GHz 802.11b radios), FHSS (frequency hopping spread spectrum), or even OFDM (orthogonal frequency division multiplexing), you should understand a little about how they work beyond the marketers hype and detractors FUD. Each has its strengths and weaknesses. None is a silver bullet. All work best in a true unobstructed line-of-sight environment. While OFDM can work in some situations without line of sight, this is not optimal, and requires an understanding of what constitutes an optimal near line of sight or even non line of sight environment. This text will not go into that detail, but will tell you that if all you can see between the near antenna and the far antenna is green (or for our northern neighbors where that white will turn to green in the summer), you have a non-optimal environment. Optimal links are over water. Very long hauls can be made over water due to refraction of the radio waves by the water. These links should run better than your calculations.

Fresnel Zone

When looking at line of sight, you must keep a few concepts in mind. While <u>you</u> might be able to see the remote antenna, your local antenna might not be able to. Radios waves in the GHz frequency range travel in straight lines, but these lines need room. Remember, these are <u>waves</u> not rays. Waves require some horizontal and vertical room while traveling. So shooting through a hole in the trees ½ a mile away will not work. The room these waves require is called a Fresnel (pronounced frah'nel) Zone. For our purposes, we calculate only the first Fresnel zone. The third and fifth also affect the signal, and for

DS they affect it negatively, while for OFDM they have a more positive effect. Anyone who's set up a long point-to-point across a hot flat expanse of desert using DSSS has probably seen this effect demonstrated very vividly.

Your Fresnel zone is a cigar-shaped area that is widest in the center. A number of wireless calculators exist on the Internet, including one linked from http://www.pananix.com/ that will calculate your Fresnel zone and more. It is difficult to envision this Fresnel zone, so if you think something might be encroaching, it probably is. If your signal strength doesn't meet your calculations (within one or two db), move your antenna(s). Your worst Fresnel environment will be shooting down a long, narrow steep-sided valley with lots of trees or through a gap between hills with similar characteristics (that hole in the trees midway between your antennas also qualifies).

SNR

A number of other things may confuse you about signal levels and SNR. Radio signals are normalized to a decibel scale. But this scale is logarithmic, not linear. SNR stands for signal to noise ratio. Ratio, in mathematics usually means divide, but since we are using a logarithmic scale, we subtract. So the difference between receive sensitivity (or noise in a high noise environment) and signal at the receiver, will translate into a signal-to-noise ratio.

What is a good SNR? Well, this will depend on a number of things. And apparently a large number of folks don't know what constitutes a good SNR. One Internet site which shall remain unnamed, has pretty colors to depict good, marginal, and unusable (green, yellow, and red respectively) signal levels. But according to this site, all my links are unusable. They show green for links over 25db SNR, yellow from 15db to 25 db, and red below 15db. Wow, I wish I could run 500W using huge dishes on my 30 miles backhauls (some of which only dream of seeing 15db and by this site are considered unusable). I consider 10 a good, solid number for calculations purposes and will run any link over 6 db without worry. While 3db might get through, 2db is a dead link, so you'd be advised to put a bigger antenna on the low SNR side. Most of my links run between 10-15 db SNR, although I have one long backhaul on a frequency I'm legally restricted to 1 W output at the antenna (EIRP – Effective Isotropic Radiated Power). This link normally sees an SNR of 7-8 during the worst part of the day and is a critical link. It has run reliably for months.

Appendix 1

StarOS Country Codes

Codes sorted alphabetically by digraph

NA	NO_COUNTRY_SET
AL	ALBANIA
AE	UNITED ARAB EMIRATES
AM	ARMENIA
AR	ARGENTINA
AT	AUSTRIA
AU	AUSTRALIA
AZ	AZERBAIJAN
BE	BELGIUM
BG	BULGARIA
BH	BAHRAIN
BN	BRUNEI DARUSSALAM
BO	BOLVIA
BR	BRAZIL
BY	BELARUS
BZ	BELIZE
CA	CANADA
CH	SWITZERLAND
CL	CHILE
CN	CHINA
CO	COLOMBIA
CR	COSTA RICA
CY	CYPRUS
CZ	CZECH REPUBLIC
DE	GERMANY
DK	DENMARK
DO	DOMINICAN REPUBLIC
DZ	ALGERIA
EC	ECUADOR
EE	ESTONIA
EG	EGYPT

ES	SPAIN
FI	FINLAND
FR	FRANCE
GB	UNITED KINGDOM
GE	GEORGIA
GR	GREECE
GT	GUATEMALA
HK	HONG KONG
HN	HONDURAS
HR	CROATIA
HU	HUNGARY
ID	INDONESIA
IE	IRELAND
IL	ISRAEL
IN	INDIA
IR	IRAN
IS	ICELAND
IT	ITALY
J1	JAPAN1
J2	JAPAN2
J3	JAPAN3
J4	JAPAN4
J5	JAPAN5
JO	JORDAN
JP	JAPAN
K2	KOREA REPUBLIC2
KP	NORTH KOREA
KR	KOREA REPUBLIC
KW	KUWAIT
KZ	KAZAKHSTAN
LB	LEBANON
LI	LIECHTENSTEIN
LT	LITHUANIA
LU	LUXEMBOURG
LV	LATVIA
MA	MOROCCO
MC	MONACO
MK	MACEDONIA
MO	MACAU
MX	MEXICO

MY	MALAYSIA
NL	NETHERLANDS
NO	NORWAY
NZ	NEW ZEALAND
OM	OMAN
PA	PANAMA
PE	PERU
PH	PHILIPPINES
PK	PAKISTAN
PL	POLAND
PR	PUERTO RICO
PT	PORTUGAL
QA	QATAR
RO	ROMANIA
RU	RUSSIA
SA	SAUDI ARABIA
SE	SWEDEN
SG	SINGAPORE
SI	SLOVENIA
SK	SLOVAK REPUBLIC
SV	EL SALVADOR
SY	SYRIA
TH	THAILAND
TN	TUNISIA
TR	TURKEY
TT	TRINIDAD & TOBAGO
TW	TAIWAN
UA	UKRAINE
US	UNITED STATES
UY	URUGUAY
UZ	UZBEKISTAN
VE	VENEZUELA
VN	VIET NAM
YE	YEMEN
ZA	SOUTH AFRICA
ZW	ZIMBABWE

Codes sorted alphabetically by country

NO_COUNTRY_SET	NA
ALBANIA	AL
ALGERIA	DZ
ARGENTINA	AR
ARMENIA	AM
AUSTRALIA	AU
AUSTRIA	AT
AZERBAIJAN	AZ
BAHRAIN	BH
BELARUS	BY
BELGIUM	BE
BELIZE	BZ
BOLVIA	BO
BRAZIL	BR
BRUNEI DARUSSALAM	BN
BULGARIA	BG
CANADA	CA
CHILE	CL
CHINA	CN
COLOMBIA	CO
COSTA RICA	CR
CROATIA	HR
CYPRUS	CY
CZECH REPUBLIC	CZ
DENMARK	DK
DOMINICAN REPUBLIC	DO
ECUADOR	EC
EGYPT	EG
EL SALVADOR	SV
ESTONIA	EE
FINLAND	FI
FRANCE	FR
GEORGIA	GE
GERMANY	DE
GREECE	GR
GUATEMALA	GT
HONDURAS	HN
HONG KONG	HK

HUNGARY	HU
ICELAND	IS
INDIA	IN
INDONESIA	ID
IRAN	IR
IRELAND	IE
ISRAEL	IL
ITALY	IT
JAPAN	JP
JAPAN1	J1
JAPAN2	J2
JAPAN3	J3
JAPAN4	J4
JAPAN5	J5
JORDAN	JO
KAZAKHSTAN	KZ
KOREA REPUBLIC	KR
KOREA REPUBLIC2	K2
KUWAIT	KW
LATVIA	LV
LEBANON	LB
LIECHTENSTEIN	LI
LITHUANIA	LT
LUXEMBOURG	LU
MACAU	MO
MACEDONIA	MK
MALAYSIA	MY
MEXICO	MX
MONACO	MC
MOROCCO	MA
NETHERLANDS	NL
NEW ZEALAND	NZ
NORTH KOREA	KP
NORWAY	NO
OMAN	OM
PAKISTAN	PK
PANAMA	PA
PERU	PE
PHILIPPINES	PH
POLAND	PL

PORTUGAL	PT
PUERTO RICO	PR
QATAR	QA
ROMANIA	RO
RUSSIA	RU
SAUDI ARABIA	SA
SINGAPORE	SG
SLOVAK REPUBLIC	SK
SLOVENIA	SI
SOUTH AFRICA	ZA
SPAIN	ES
SWEDEN	SE
SWITZERLAND	CH
SYRIA	SY
TAIWAN	TW
THAILAND	TH
TRINIDAD & TOBAGO	TT
TUNISIA	TN
TURKEY	TR
UKRAINE	UA
UNITED ARAB EMIRATES	AE
UNITED KINGDOM	GB
UNITED STATES	US
URUGUAY	UY
UZBEKISTAN	UZ
VENEZUELA	VE
VIET NAM	VN
YEMEN	YE
ZIMBABWE	ZW

Appendix 2

Network Primer

Introduction

This appendix is intended to aid novice network technicians understand and build a routed network. This text will not be all-encompassing, but is intended to get you over the initial hurdle of subnetting and routing an IPv4 network.

Background

For those who have been assigned a “Class C” network by their providers, but don't know where to go from here, this text will provide that help. It is really simple once you understand.
First, I'd like to point out that us “old-timers” still use the terms Class A, Class B, and Class C when referring to network blocks. Understand, however, that these Classes were made obsolete around 1996 when Classless Inter Domain Routing (CIDR) was standardized. This text will not discuss CIDR, but will restrict itself to the subset of CIDR in use globally known as Variable Length Subnet Masking (VLSM).
To understand VLSM, it is important to grasp where this concept comes from. So first we'll delve lightly into IPv4 and just how an IP address is composed, and from there we'll be able to see how VLSM works.
After understanding how VLSM works, we'll look at how to easily subnet your “Class C” address block. Basically, if you can multiply and divide by 4, 8, 16, 32, 64, and 128 numbers from 1-255, you've got it made.

IP

IP addresses are composed of 4 decimal digits separated by dots. This notation is called “dotted decimal notation”. Each set of decimal numbers can range from 0 to 255. The astute student will note that this equates in binary to the numbers from 00000000 to 11111111. Note that this is eight places in binary. So each number is sometimes referred to as an “octet”.
Nothing difficult here. All we have to do is think of each number (0-255) as a binary octet.
If you translate each octet to its binary form from decimal, you remove the decimal dots between the octets and translate the entire number into decimal, you will get a unique decimal number equivalent to the IP address. While this is not a necessary exercise to accomplish, it will help you understand how

these numbers are derived. Additionally, these unique decimal numbers can also be used by your web browser in the URL bar. But the reason we use IP addresses in dotted decimal notation is to help network admins better "see" the contiguous parts of the network (i.e., which IPs are neighbors and which aren't). It's rather obvious looking at an IP address which IPs are neighbors because on a Class C network, if the first three octets are the same, then obviously, IPs different only in the last octet are neighbors. That is 192.168.1.1 and 192.168.1.254 are neighbors on their Class C network because the first three octets are the same. This means that these two IPs can talk to each other directly without need of a gateway. IPs that are not neighbors (not on the same subnet), cannot talk to each other directly, but need to go through a gateway. The two Class C addresses 192.168.1.1 and 192.168.2.1 are not neighbors and require a gateway in order to communicate.

NETMASK

This brings us to the concept of a netmask. **A netmask defines the network.** That is, the netmask defines which IPs are neighbors and can talk directly to each other, and which IPs are not neighbors and therefore must use a gateway to access a non-neighbor IP.

Under the obsolete Classful concept, netmasks were one of 255.255.255.0, 255.255.0.0, or 255.0.0.0. The 255's indicated the network portion of the IP, and the zeros indicated the host (neighbor) portion of the IP. If the network octets matched (192.168.1.x), then the hosts were neighbors and could talk directly to each other.

Note that under the classful concept of a network, netmask numbers were either 255 or 0. That is, the binary representation was an octet full of ones or zeros. But to implement CIDR, we must now allow for other representations. The network part of an IP is still represented in binary by ones and the host portion by zeros, but the ones and zeros no longer stop neatly at the decimal places. This means that we can have numbers other than 255 and zero, but that the binary representation will still have a definitive dividing point. That is, when the netmask is translated from decimal into binary notation, under VLSM we will have binary ones to the left, then zeros to the right. We will have no binary ones to the right of the first zero. (Note: CIDR does not carry this limitation, but a non-VLSM netmask is an academic exercise only – unless you are either crazy or masochistic.).

What the above paragraph means is that a valid VLSM netmask will contain a 255 followed by any one of 255, 254, 252, 248, 240, 224, 192, 128, or 0, and if that number is not 255, then any subsequent numbers must be zero. This is because if you translate the aforementioned decimal numbers to binary, you can clearly see ones to the left, zeros to the right:

255: 11111111
254: 11111110
252: 11111100
248: 11111000
240: 11110000
224: 11100000
192: 11000000
128: 10000000

0: 00000000
So we can have a netmask that looks like: 255.255.255.224, or 255.255.248.0, or 255.240.0.0. But we cannot have 255.0.240.0 or any decimal number not listed above (e.g., 255.255.255.220).

VLSM Notation

Along with the use of VLSM and netmasks composed of other than 0 and 255, a new convention was designed to more easily denote these new VLSM subnets. This VLSM notation is nothing more complicated than counting the number of ones in the netmask and showing how many there are. This notation can be used in lieu of a netmask as follows:
if we have a netmask of 255.255.255.0, we can see that this is 3 octets of 8 ones in binary. So an IP address can be said to be 192.168.1.1 netmask 255.255.255.0 or 192.168.1.1/24. The /24 tells you how many ones are in the network portion of the netmask. So a netmask of 255.255.255.240 is the same as a /28. The /28 is often called a suffix because it is suffixed to the IP address in lieu of the netmask. Since there are a total of 32 bits in an IPv4 IP address, we can see that there are 4 zeros (32 – 28 = 4). Now it just so happens that 4 ones in binary (1 1 1 1) == 16. It's not a coincidence that a /28 network (netmask 255.255.255.240) will give you exactly 16 IPs in that subnet. Subtract one IP for the network, one for the broadcast address and you have 14 host IPs. You'll need to use one IP for your gateway router, so now have 13 IPs to use for your hosts (clients).
This means that a netmask 255.255.255.248 or /29 suffix has 3 binary places or 8 IPs, and a netmask of 255.255.255.224 or /27 has 5 binary places or 32 IPs.
Remember I told you all you had to be able to do was multiply and divide by 2, 4, 8, 16, 32, 64, or 128 to subnet? The reason should start becoming clear:

Netmask		Last octet in binary		suffix	# IPs
255.255.255.0	==	00000000	==	/24 ==	256
255.255.255.128	==	10000000	==	/25 ==	128
255.255.255.192	==	11000000	==	/26 ==	64
255.255.255.224	==	11100000	==	/27 ==	32
255.255.255.240	==	11110000	==	/28 ==	16
255.255.255.248	==	11111000	==	/29 ==	8
255.255.255.252	==	11111100	==	/30 ==	4
255.255.255.254	==	11111110	==	/31 ==	2 (unusable)
255.255.255.255	==	11111111	==	/32 ==	1

Subnetting

To subnet, we will just take a netblock we have and carve it up. We can carve up a full “Class C” into 2 /25 networks, or 4 /26 networks, or 8 /27 networks, or 16 /28 networks, or 32 /29 networks. But we don't have to restrict ourselves to dividing them up in just one way. We may need two /27 subnets, 4 /28 subnets, and whatever is left as one contiguous block. So we begin.

It's easiest to start at one end or other of the netblock and start carving out the biggest chunks first. So our first two blocks will be the two /27 netblocks. The first is too easy:
192.168.1.0/27. == 192.168.1.0-192.168.1.31.
Then we have:
192.168.1.32/27 == 192.168.1.32-192.168.1.63.
Remember, the .0 and .32 addresses are the network addresses; the .31 and .63 are the broadcast addresses. It's best to pick a policy for how to set your gateways. This can be either the first or last usable address in a subnet. I like to use the first, so the gateways will be 192.168.1.1 and 192.168.1.33. The rest are open for clients. We can continue to carve up our network, subnetting to suit our needs.

Adjacent and Contiguous

When we received our netblock, it was one contiguous block. That is, it went from the first to last IP with no subnetting. All the IPs were on the same subnet. After carving them up, we had IPs, some of which were now in adjacent subnets.
Looking at our network and the changing demands, we now see we need to open up a particular subnet and combine two adjacent networks into one contiguous block again. But can we do this? The answer is a qualified, yes.
The question is not whether we can combine two adjacent blocks into one contiguous block or not, the question is how much we have to open up the netmask to accomplish this.
So let's take two examples. The first one is easy. We have two netblocks:
192.168.1.112/29
192.168.1.120/29
The suffix tells us we have 3 binary places (32 – 29 = 3), which is the same as 2^3 (2 raised to the 3d power – i.e., 2 cubed) or 8.
Now the network address we want to eliminate is 120. If you divide 120 by 8 you get 15. Because 15 is an odd number, we can combine these two subnets into one /28. Checking our math, 2^4 power is 16. If we divide 120 by 16, we get 7 with a remainder of 8. And 16 times 7 equals 112. This confirms that 112 will be our network address, and that 120 cannot be. So we can combine 192.168.1.112/29 and 192.168.1.120/29 into 192.168.1.112/28.
Before we go any farther, let's make sure we understand the rules for combining adjacent networks:

1. The adjacent networks must be the same size. You cannot combine two adjacent networks of unequal size.
2. If the upper network's network IP is divisible by the current number of IPs and the division results in an odd number, or if divided by the twice the current number of IPs and results in a number with a remainder, then you can combine the networks. Otherwise, you can't.

The next example will show the above rules more clearly. We have two networks:
192.168.1.48/28
192.168.1.64/28

These two networks have 16 IPs each (2^(32-28)). If we divide the upper network's network address by 16, we get 64 / 16 = 4. This number is even and tells us that opening our subnet (i.e., changing our subnet to a /27) will not allow these two subnets to be combined. In fact, if the 192.168.1.64 was opened even further, it would only continue to expand upward, not down into the original 192.168.1.48 network: 64 / 32 = 2. It is only when we get to a /25 suffix, do the two networks in this example combine. By then we have a subnet of 128 IPs.

Finding the network

For those of you who still haven't quite caught on, we can identify the network and broadcast address of any network given only the IP and the suffix. Let's try an example:
192.168.1.195/27.
First find the number of IPs:
32-27=5
2^5=32
So we have 32 IPs. You could just count it out: 2 – 4 – 8 – 16 – 32. Extend five fingers one at a time doubling the number as you go.
Now, just divide 195 by 32 == 6 remainder 3.
Using only the 6 and multiplying by the number of IPs, we get:
6 * 32 = 192. So our network address is 192.168.192/27.
To find our broadcast address, we get the next network address and subtract 1:
7 * 32 = 224; 224 – 1 = 223. So our broadcast address is 192.168.1.223.

Routing

It doesn't do much good to break your network up into tiny little pieces if you don't know what to do with the pieces afterward. So here's how this will play out. This is based on an actual network, and you may or may not see the sense in doing it this way. Remember, if it works, it's not wrong. But I like to keep things logical. And since this is my network, here are my rules:
I have several /27 networks to distribute to remote radios. They are:
10.10.1.32/27
10.10.1.64/27
10.10.1.96/27
While I could keep going, the principal will be the same. My distribution scheme goes like this:
From my principal router, I use 192.168.255.0/24 for local routing. The radio links use 172.16.#.0/24 to route over the air. I have 3 radios on my roof each talking to a different remote radio. The remote radios will be APs that will route to the client radios. Client radios will do NAT routing so clients can have as many systems as they want.

On my principal router I have:
Point-to-point frame relay to my provider (pvc0)
ethernet for local distribution and routing (eth0)
ifconfig shows me:
pvc0: 169.254.19.13/30
eth0: 10.10.1.1/27
eth0:1 192.168.255.1
routing table looks like this:

10.10.1.0/27	10.10.1.1
10.10.1.32/27	192.168.255.2
10.10.1.64/27	192.168.255.3
10.10.1.96/27	192.168.255.4
0.0.0.0/0	169.254.19.14

What the above says is that the network 10.10.1.0/27 is routed locally. Each of the other 10.10.1.x/27 networks routes to a different radio with IPs on the 192.168.255.0/24 subnet. Default route is out the frame relay.

Each radio is similar, so looking at one pair of radios is the same as looking at any other pair, just with slighly different numbers. So the radio 192.168.255.2 on its ethernet interface has no bridges and has wpc1 of 172.16.2.1. The routing table shows default (0.0.0.0/0) route of 192.168.255.1, and has the network 10.10.1.32/27 routed to IP 172.16.2.2. (Radios 2 and 3 have IPs 192.168.255.3 and 4 and use networks 172.16.3.0/24 and 172.16.4.0/24 respectively for routing).

The remote radio has a wpci1 interface of 172.16.2.2 and the ethernet and wpci2 interfaces are bridged and have an IP of 10.10.1.33. Routing table has only the default route of 0.0.0.0/0 pointing to 172.16.2.1.

Each client radio has an external wpci1 interface on the 10.10.1.32/27 network with default route (0.0.0.0/0) pointing to 10.10.1.33. All clients use 192.168.100.0/24 as their internal network, NAT to the external interface, and have dhcp server turned on for their use internally.

The above network is exceedingly easy to expand and can grow without limits. Its implementation is incredibly easy. Client radios are different only in their external IPs, so only one configuration file is required and the IP and ESSID changed.

KISS: keep it stupid, simple, is my motto. And by using the above scheme, life is very easy.

Final note: With the exception of the IPs in the 10.10.1.0/24 range, which are really public IPs on my network, and the frame relay IP, this is a portion of my 20 radio network. Longest chain is 4 radios up through mountainous terrain. All radios have one or more AP interfaces and one or more backhaul

interfaces. While the number of clients I service is small (less than 200), the network covers over 900 square miles.